

الحماية الجنائية لسرية المعلومات الإلكترونية

دراسة مقارنة

محمد كمال محمود الدسوقى

ماجستير فى القانون وباحث دكتوراه

دار الفكر والقانون

٢١ شارع السعيد الشرقاوى حى الجامعة
أمام القرية الأولمبية - المنصورة

تليفون: ٠٥٠٢٢٣٦٢٨١ محمول: ٠١٠٠٦٠٥٧٧٦٨

الحماية الجنائية لسـرية

المعلومات الالكترونية

دراسة مقارنة

محمد كمال محمود الدسوقي

ماجستير في الحقوق وباحث دكتوراه

طبعة 2021

دار الفكر والقـانون

للنشر والتوزيع

21 ش السعيد الشرقاوي – حي الجامعة – أمام القرية الأولمبية - المنصورة

تليفاكس : 0020502235671 تليفون : 0502236281

محمول 00201006057768

اسم الكتاب : الحماية الجنائية لسرية المعلومات الالكترونية

اسم المؤلف: محمد كمال محمود الدسوقي

الطبعة الأولى

سنة الطبع : 2021

رقم الإيداع بدار الكتب المصرية : 14621

الترقيم الدولي: 978-977-747-018-6

الناشر

دار الفكر والقانون للنشر والتوزيع

21 ش السعيد الشرقاوي – حي الجامعة – أمام القرية الأوليمبية - المنصورة

فاكس : 0020502363767 تليفون : 0502236281

محمول 00201006057768

00201119339442

dar.elfker@Hotmial.com

المحامي / أحمد محمد أحمد سيد أحمد

قال اللـه تعالى:

(يَا أَيُّهَا الَّذِينَ آمَنُوا اجْتَنِبُوا كَثِيرًا مِنَ الظَّنِّ إِنَّ بَعْضَ الظَّنِّ إِثْمٌ وَلَا تَجَسَّسُوا)

(الحجرات : 12)

(يَا أَيُّهَا الَّذِينَ آمَنُوا لَا تَدْخُلُوا بُيُوتًا غَيْرَ بُيُوتِكُمْ حَتَّى تَسْتَأْنِسُوا وَتُسَلِّمُوا عَلَى أَهْلِهَا ذَلِكُمْ خَيْرٌ لَكُمْ لَعَلَّكُمْ تَذَكَّرُونَ فَإِنْ لَمْ تَجِدُوا فِيهَا أَحَدًا فَلَا تَدْخُلُوهَا حَتَّى يُؤْذَنَ لَكُمْ وَإِنْ قِيلَ لَكُمُ ارْجِعُوا فَارْجِعُوا هُوَ أَزْكَى لَكُمْ وَاللـهُ بِمَا تَعْمَلُونَ عَلِيمٌ)

(النور : 27-28)

الإهداء

إلى أمي

منبع الآمال ، نبع الحنان ، التي أجهدت نفسها لأجلي بلا ضجر، لطالما أردت أن أوفيها بعض من حقها، ولكنني أعلم بأن حقها أعظم مما أملك من كلام أو هدايا ، رعاها المولى وجزاها من الثواب أجزاه.

إلى أبي

قدوتي الأولى ونبراسي الذي ينير دربي ، والذي أعطاني ولم يزل يعطيني بلا حدود ، من رفعت رأسي عاليًا افتخارًا به ، وفقه الله ورعاه وسدد على الخير خطاه.

وإلى أخوتي وعائلتي سندي وعزوتي

وإلى روح من أضاء بعلمه عقل غيره ، وأظهر بسماحته تواضع العلماء **الدكتور عبد الحميد عثمان** ، أسأل الله العظيم أن يغفر له ويرحمه، وأن ينفعه بما علمنا

ثم إلى كل من علمني حرفًا أصبح سنا برقه يضيء الطريق أمامي

كما أهدي هذا العمل إهداء خاص إلى أغلى وأقرب الناس إلى قلبي زوجتي الحبية **منى مسلم**

المقدمة

أولا: موضوع البحث:

يعد استخدام التكنولوجيا في تخزين المعلومات وتصنيفها واسترجاعها ونقلها، من الركائز الرئيسة التي تعتمد عليها غالبية المجتمعات في العصر الحديث، نظراً للفوائد الكبيرة لتلك التكنولوجيا أبرزها ضمان سرعة نقل وتبادل المعلومات من مختلف أنحاء العالم والحصول عليها بسهولة،وبأقل جهد ووقت وتكلفة، ونظراً لتلك المزايا فإنه يوماً بعد يوم يتنامى الاعتماد على تكنولوجيا المعلومات في مختلف المجالات العلمية والعملية. ونتيجة لذلك أصبحت النظم المعلوماتية والحاسبات الآلية مستودعاً لكمٍ هائل وضخم من البيانات والمعلومات الشخصية، والاقتصادية، والمالية،والعسكرية،وأصبحت الشبكات الإلكترونية ممراً لنقل كمٍّ هائلٍ من تلك المعلومات من مركزها إلى مختلف أنحاء العالم.

وعلى الرغم من الإيجابيات المتقدمة لتكنولوجيا المعلومات، إلا أن التهديدات التي تتعرض لها المعلومات المعالجة أو المخزنة أو المنقولة إلكترونياً والتي تمس بسلامتها وسريتها وتوافرها، باتت أخطر وأكثر مما كان عليه الحال بالنسبة للوسائل التقليدية المستخدمة في هذا المجال نتيجة لإساءة استخدام هذه التكنولوجيا من قبل البعض للوصول إلى المعلومات والتجسس عليها واعتراضها أثناء انتقالها. وأمام تلك المخاطر والتهديدات واتساع نطاقها لجأت الدول إلى حشد الجهود الدولية والإقليمية والوطنية لدرء تلك المخاطر والتصدي لها فنياً وتشريعياً، في محاولة للموازنة بين حاجات المجتمع لجمع وتخزين ومعالجة البيانات الكترونيا، وضمان حماية هذه البيانات من مخاطر الاستخدام غير المشروع لتقنيات معالجتها، وعلى وجه الخصوص سرية المعلومات.

وحيث أن سرية المعلومات من أهم صور الحماية التي ينشدها مستخدموا

أنظمة الحاسب الآلي وشبكات المعلومات، نظرا لما تشكله هذه المعلومات من قيمة، تجعلها هدفا للاعتداء بصفة مستمرة، لذلك جاء اختيارنا لموضوع البحث: " الحماية الجنائية لسرية المعلومات الإلكترونية (دراسة مقارنة) "

ثانيا: أهمية البحث:

تتجلى أهمية هذا البحث في كونه يتعلق بمطلب أساسي ينشده جميع مستخدمي تكنولوجيا المعلومات أفراداً ومؤسسات وهيئات، وهو ضمان سرية معلوماتهم التي تحتويها النظم المعلوماتية،في الوقت الذي يتنامى فيه الاعتماد على الحاسبات الآلية وشبكات الاتصال في جمع ونقل المعلومات والبيانات الخاصة بالأشخاص الطبيعيين والأشخاص المعنويين، وتخزينها ومعالجتها وتحليلها، وظهور نظام بنوك المعلومات (Data Bank) والتي يقصد بها " تكوين قاعدة بيانات تفيد موضوعا معينا وتهدف لخدمة غرض معين، ومعالجتها بواسطة أجهزة الحاسبات الإلكترونية؛ لآخراجها في صورة معلومات تفيد مستخدمين مختلفين في أغراض معينة"[(1)] كبنوك معلومات الشركات المالية والبنوك، وبنوك المعلومات الوطنية التي تتضمن معلومات خاصة عن الأفراد مثل حالتهم الصحية والعائلية وانتماءاتهم السياسية والعرقية والدينية،حيث باتت المعلومات المخزنة في تلك النظم عرضة لمخاطر إساءة الاستخدام، والوصول إليها بطريق غير مشروع أكثر من أي وقت مضى إذا ما تم مقارنتها بالوضع التقليدي الذي كانت تدون فيه المعلومات والبيانات في سجلات ورقية وتحفظ في خزائن خلف أبواب مغلقة. كما أن شيوع (النقل الرقمي) للمعلومات عبر شبكات الاتصال الداخلية أو المحلية أو العالمية أدّى إلى تسهيل عمليات التجسس الإلكتروني، نتيجة لعدم قدرة شبكات الاتصال على توفير الأمان الكامل لسرية ما ينقل عبرها من معلومات وبيانات، فضلا عن إمكانية استخدام هذه الشبكات كوسيلة للوصول الغير مشروع للمعلومات عن بعد والحصول عليها.

---

(1)د.علاء عبدالباسط خلاف – الحماية الجنائية للحاسب الإلكتروني والإنترنت في ضوء قانون العقوبات وقانون الاجراءات الجنائية وقانون حماية حقوق الملكية الفكرية بجمهورية مصر العربية- معهد الكويت للدراسات القضائية والقانونية- الطبعة الثانية 2008/2007- صـ 131

وقد كشفت دراسات قدمت في مؤتمر متخصص استضافته القاهرة، أن جريمة تحدث كل ثلاث دقائق على شبكة الإنترنت التي تضم 500 مليون موقع وأكثر من 15 بليون صفحة وملايين قواعد المعلومات وغيرها. ويقدر الخبراء قيمة الخسائر المادية للاعتداءات الإلكترونية على حقوق الملكية الفكرية بنحو 72 بليون دولار سنويا[1]. وبالنسبة لمملكة البحرين فإنه وفقا لإحصائية قضايا شعبة مكافحة الجرائم الإلكترونية بوزارة الداخلية[2] بلغت إجمالي البلاغات الخاصة بالجرائم الإلكترونية في عام 2008حوالي 73 بلاغاً، وفي عام 2009 حوالي 103 بلاغاً، وفي عام 2010 حوالي 139 بلاغاً، وفي عام 2011 حوالي 249 بلاغاً. وبالنسبة لعدد الجرائم الماسة بسرية المعلومات فإن عددها وفقاً للإحصائية السابقة كالآتي:

السنة	نوع الجريمة	عدد البلاغات
2008	سرقة البريد الإلكتروني والاختراق	6
2009	سرقة البريد الإلكتروني واختراق	30
2010	سرقة البريد الإلكتروني واختراق	23
2011	سرقة البريد الإلكتروني واختراق	35

كما يستمد موضوع البحث أهميته لما له من انعكاسات هامة من الناحية العملية على بيئة التعاملات الإلكترونية في جميع دول العالم ومنها مملكة البحرين، كالتعاملات الإلكترونية في المجال التجاري والمصرفي، وفي المجال الإداري مثل الحكومة الإلكترونية، خاصة وأن مملكة البحرين قد قطعت شوطاً كبيرا في مجال الخدمات الإلكترونية، واحتلت المركز الـ13 عالمياً والأول خليجيا وعربيا في مجال الخدمات الإلكترونية وفقا لمؤشر الأمم المتحدة للحكومة الإلكترونية لسنة 2010[3]، وتتطلع وفقا لاستراتيجية الحكومة الإلكترونية 2007 –

---

(1) تقرير منشور على موقع مركز الأهرام للدراسات السياسية والاستراتيجية http://acpss.ahram.org.eg

(2) إحصائية صادرة عن وزارة الداخلية بمملكة البحرين - غير منشورة.

(3) الخبر منشور على موقع وكالة أنباء البحرين بتاريخ 2011/02/14 :

-http://www.bna.bh/portal/news/447185

2010 إلى الريادة في مجال الحكومة الإلكترونية[1]،وتسعى إلى تقديم جميع الخدمات الأساسية وتوفيرها إلكترونيا وإتاحتها لجميع الأفراد والمؤسسات الحكومية والتجارية وزيادة رضائهم عن الخدمات التي تقدمها ، وهو ما يتطلب تطوراً تشريعياً موازياً يوفر الحماية القانونية اللازمة للمعلومات والبيانات التي يقدمها الأشخاص والمؤسسات بمناسبة استخدام إحدى الخدمات التي تقدمها الحكومة الإلكترونية لما قد تتعرض له من أخطار أهمها المساس بسريتها ، إذ إن توفير مثل هذه الحماية يشكل عاملاً مشجعاً للأفراد والمؤسسات والهيئات للإقبال على الخدمات التي تقدمها الحكومة الإلكترونية وبالتالي تحقيق الأهداف المرجوة من ورائها.

لذلك تعد هذه الدراسة من طائفة الدراسات التي تنصب على الجرائم المستحدثة، وهو أحوج ما يحتاج إليه المشرع للاستفادة منها عند وضع تنظيم قانوني ولاسيما في ظل غياب هذا التنظيم للجرائم المعلوماتية والجرائم الماسة بسرية المعلومات الإلكترونية على وجه التحديد ، بما يسهم في تطوير الرؤى التشريعية وكذلك القضائية.

ثالثا: مشكلة البحث:

كما أشرنا سالفا فإن موضوع هذا البحث يتناول مطلباً أساسياً ينشده جميع مستخدمي تكنولوجيا المعلومات أفراداً كانوا أو مؤسسات ، وهذا المطلب يتمثل في ضمان الحق في الخصوصية بتوفير الحماية الجنائية لسرية المعلومات الإلكترونية ، وخاصة في مجتمعٍ يعتمد في بيئته الواقعية على تقنية أنظمة المعلومات، ويدير شؤونه ومرافقه بواسطة هذه التقنية.

ومن هذه النقطة يثار التساؤل العلمي بشأن قدرة النظام القانوني البحريني على مواجهة تلك الجرائم في حالة وقوعها بحالته التي هو عليها ؟ وبمعنى آخر هل النصوص العقابية التقليدية كفيلة بالتصدي للجرائم الماسة بسرية

---

(1)استراتيجية الحكومة الإلكترونية 2007 – 2010 منشورة على موقع بوابة الحكومة الإلكترونية www.e.gov.bh.

المعلومات الإلكترونية، أم أنها بحاجة إلى تطوير وتعديل بحيث تشمل كل صور الأفعال الإجرامية لتلك الجرائم ؟ أم أنه من الأفضل إصدار تشريع خاص بالجرائم المعلوماتية بما فيها الجرائم الماسة بسرية المعلومات الإلكترونية؟ وما هي سبل مكافحة تلك الجرائم ؟ تلك الإشكالات والموضوعات ستكون مناط بحثنا ونسأل الله التوفيق والسداد في معالجتها.

رابعاً: أهداف البحث:

نسعى من خلال هذا البحث إلى تحقيق مجموعة من الأهداف أهمها ما يأتي:

1. التعرف إلى الإطار القانوني للجرائم الماسة بسرية المعلومات الإلكترونية، والتعرف إلى الجهود المحلية والإقليمية والدولية المبذولة في سبيل مكافحتها.

2. اقتراح الوسائل القانونية لمكافحة هذه الجريمة.

3. المساهمة في تطوير البنية التشريعية وكذلك القضائية

4. إغناء المكتبة القانونية بالمستجد من المعلومات والأحكام القضائية المتعلقة بهذا الموضوع وتمكين الدارسين والباحثين والمختصين من الإفادة منها.

خامسا: منهجية البحث:

تتمثل مشكلة البحث الرئيسة في المواجهة التشريعية للجرائم الماسة بسرية المعلومات الإلكترونية، وذلك من خلال دراسة الأحكام القانونية الخاصة بالجرائم المعلوماتية، وفحص قدرة النصوص العقابية القائمة على توفير الحماية القانونية اللازمة لسرية المعلومات الإلكترونية، وعلى ذلك سنعتمد المنهج التوفيقي والذي يجمع بين التحليل والتأصيل والمنهج الوصفي المقترن بالمنهج التحليلي في هذا البحث، والذي سيعتمد على تحديد ومن ثم تحليل الجرائم الماسة بسرية المعلومات الإلكترونية، ومعرفة أسبابها ووسائل ارتكابها، ثم نقترح سبل مكافحتها.

كذلك سنستخدم المنهج المقارن، والذي سنسلط من خلاله الضوء على الجرائم المعلوماتية الماسة بسرية المعلومات الإلكترونية في عدة نظم تشريعية وقضائية تساعدنا على فهم أوسع وأعمق للتنظيم القانوني المناسب لها.

الفصل الأول

الجرائم المعلوماتية الماسة بسرية المعلومات الإلكترونية

تتعدد المخاطر والجرائم التي يمكن أن تتعرض لها المعلومات في إطار البيئة الإلكترونية والتي تستهدف عناصرها السرية وسلامتها وديمومتها وتوفرها، ومن أبرز صور تلك الجرائم: الدخول غير القانوني (غير المصرح به) ، الاعتراض غير القانوني، تدمير المعطيات، اعتراض النظم، وغيرها.

وسنبحث في هذا الفصل الجرائم المعلوماتية التي تستهدف عناصرسرية المعلومات الإلكتروني وهي جرائم الدخول غير القانوني (غير المصرح به) ، الاعتراض غير القانوني، والتي تشكل تهديداً خطيراً لأمن المعلومات البيانات الإلكترونية.

وبغية تناول الموضوع من جوانبه كافة نتولى في هذا الفصل التعريف بالجريمة المعلوماتية من حيث ماهيتها وخصائصها والتعريف بالمجرم مرتكب هذه الجرائم وسماته وفئاته في المبحث الأول، ثم نتناول ماهية سرية المعلومات الإلكترونية في المبحث الثاني، بينما سنتناول في المبحث الثالث صور الجرائم المعلوماتية الماسة بسرية المعلومات الإلكترونية من حيث بيان مفهوم كل جريمة منها وأركانها ووسائل ارتكابها وموقف التشريع البحريني منها.

المبحث الأول

ماهية الجريمة المعلوماتية

تعد الجرائم الماسة بسرية المعلومات الإلكترونية، إحدى صور الجرائم المعلوماتية وإحدى تطبيقاتها، لذا فمن الضروري قبل الخوض في موضوع هذا البحث استعراض مفهوم الجريمة المعلوماتية، والخصائص المميزة لها، والتعرف على خصائص شخصية المجرم المعلوماتي، وفئاته.

المطلب الأول

مفهوم الجريمة المعلوماتية

اختلف الفقهاء والشراح حول مفهوم الجريمة المعلوماتية ، ومرد ذلك إلى الطريقة التي تناول بها كل فقيه الجريمة المعلوماتية والمعيار الذي اعتمده في تعريفها. وسوف نستعرض في هذا المطلب الآراء الفقهية المختلفة لتعريف هذه الجريمة.

يذهب البعض إلى تعريف الجريمة المعلوماتية بأنها نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسب أو التي تحول عن طريقه[1].

يستند التعريف السابق إلى موضوع الجريمة وصور السلوك المادي المُجَّرم، ويؤخذ عليه أنه يضيق من مفهوم الجريمة المعلوماتية حيث أنه يخرج طائفة من الأفعال غير المشروعة يستخدم فيها الحاسوب كأداة لارتكابها كالاحتيال المعلوماتي. فضلا عن أن قصرتعريف الجريمة المعلوماتية على عدة صور للسلوك المادي للجريمة، قد يؤدي إلى خروج بعض الأفعال الآخرى التي لم يشملها التعريف من نطاق التجريم مثل الأفعال التي تستهدف الشبكات والمواقع الإلكترونية بقصد إعاقة الاتصال، وانتقال، المعلومات ومنع الوصول

---

(1) تعريف الاستاذ (Rosenblatt)، مشار اليه لدى د. يونس عرب - موسوعة القانون وتقنية المعلومات - دليل أمن المعلومات والخصوصية - جرائم الكمبيوتر والإنترنت - الجزء الأول ، منشورات إتحاد المصارف العربية ، الطبعة الأولى ، ص 213

للمعلومات، والحرمان من الخدمة الإلكترونية بشكل عام.

بينما يستند البعض الآخر في تعريفه للجريمة المعلوماتية إلى وسيلة ارتكابها وهو الحاسوب، فيعرفها بأنها: فعل إجرامي يستخدم الكمبيوتر في ارتكابه كأداة رئيسة[1].

وهذا التعريف منتقد من حيث أن تعريف الجريمة ينبغي أن يكون جامعاً لعناصرها وليس مقتصراً على وسيلة تحقيقها.

ويعرفها البعض بأنها (عمل أو امتناع يأتيه الجاني إضرارا بمكونات الحاسب وشبكات الاتصال الخاصة به، التي يحميها قانون العقوبات ويفرض له عقابا)[2]

وذهب خبراء متخصصون من بلجيكا إلى أن (جريمة الكمبيوتر) هي (كل فعل أو امتناع عمدي ينشأ عن الاستخدام غير المشروع لتقنية المعلوماتية ويهدف إلى الاعتداء على الأموال المادية أو المعنوية)[3]

وقد عرفت منظمة التعاون الاقتصادي والتنمية (OECD) Organization for Economic Co-operation and Development الجريمة المعلوماتية بأنها (كل فعل أو امتناع من شأنه الاعتداء على الأموال المادية أو المعنوية يكون ناتجا بطريقة مباشرة أو غير مباشرة عن تدخل التقنية المعلوماتية)[4]

كما تبنى مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاقبة المجرمين والذي

---

(1) تعريف الأستاذ (Eslie D. Ball)، مشار اليه لدى د. يونس عرب - صور الجرائم الإلكترونية واتجاهات تبويبها - هيئة تنظيم الاتصالات مسقط - سلطنة عمان ورشة عمل تطوير التشريعات في مجال مكافحة الجرائم الإلكترونية 2-4 نيسان / إبريل 2006 صـ3 - منشورعلى الموقع الالكتروني:

www.ituarabic.org/coe/2006/E-Crime/Documents%20and%20Presentations/DAY%201/Doc3-Jor.DOC

(2) د. محمد على العرين ، الجرائم المعلوماتية - دار الجامعة الجديدة للنشر - الإسكندرية 2011 - صـ 56

(3) عفيفي كامل عفيفي - جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون دراسة مقارنة - منشورات الحلبي الحقوقية بيروت- لبنان- صـ32

(4) د. هشام محمد فريد رستم - قانون العقوبات ومخاطر تقنية المعلومات - 1995 - مكتبة الآلات الكاتبة - أسيوط - مصر صـ34

عقد في فينا في سنة 2000م تعريفا للجريمة المعلوماتية حيث عرفها بأنها (أية جريمة يمكن ارتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية أو داخل نظام حاسوب، وتشمل تلك الجريمة من الناحية المبدئية، جميع الجرائم التي يمكن ارتكابها في بيئة الكترونية)[1]

وفي تقديري يعد هذا التعريف من أكثر التعريفات شمولية إذ تناول الجريمة المعلوماتية من جوانبها المختلفة أي سواء كان النظام الحاسوبي أو الشبكة هو الوسيلة أو هو الهدف من ارتكابها، كما جاء التعريف عاما ليشمل جميع الجرائم المعلوماتية أيا كانت صورها والتي تتطور أنماطها يوما بعد يوم.

---

(1) محمد أمين احمد الشوابكة – جرائم الحاسوب والإنترنت (الجريمة المعلوماتية) – دار الثقافة -عمان،الأردن 2004 - صـ10

المطلب الثاني

خصائص الجريمة المعلوماتية

تتسم الجريمة المعلوماتية بأنها جريمة مستحدثة ومختلفة من حيث محلها ونطاقها ومخاطرها، ووسائل ارتكابها، والمشكلات الناجمة عنها، فهي تتميز بطبيعة خاصة وتتمتع بعدة خصائص تميزها عن الجريمة التقليدية أهمها ما يأتي:

1- تستهدف الجرائم المعلوماتية معنويات لا ماديات، فالجريمة المعلوماتية تستهدف المعلومات وهي أشياء معنوية غير محسوسة.[1]

2- صعوبة إثبات واكتشاف الجرائم المعلوماتية مقارنة بالجرائم التقليدية،حيث يصفها البعض بأنها إجرام خفي حيث يأتي الجاني جريمته في الخفاء، وبالتالي يصعب ضبطه، وأنها جريمة معقدة يتسم مرتكبها بالذكاء والاحتراف، لذا فالجريمة تكون أكثر تعقيدا وبالتالي قد يصعب معرفة أو اكتشاف مرتكبها.[2]، وفضلاً عما تقدم فإن صعوبة إثبات واكتشاف الجرائم المعلوماتية يمكن إرجاعه إلى الأسباب الآتية:

أ) أن جزءاً كبيراً من الأدلة غير ملموس ويزول بسرعة، ويرجع ذلك إلى أن أنواع العناوين الإلكترونية وبيانات حركة المرور تخزن في ذاكرة النظام الحاسوبي لمدة قصيرة ولا تخزن بشكل دائم.[3]

ب) إذا ما تم العثور على تلك الأدلة فإنه من السهولة إتلافها من قبل الجناة. فضلا عن أن غياب الاعتراف القانوني بطبيعة تلك الأدلة يعد من أهم عوائق الإثبات.[4]

ج) لجوء مرتكبي الجرائم المعلوماتية إلى استخدام وسائل وأساليب متجددة

---

(1) د.يونس عرب - صور الجرائم الإلكترونية واتجاهات تبويبها- مرجع سابق - صـ 7

(2) نسرين عبدالحميد نبيه- الجريمة المعلوماتية والمجرم المعلوماتي- منشأة المعارف - الإسكندرية 2008 - صـ 4

(3) ورقة عمل بعنوان (تدابير لمكافحة الجرائم المتصلة بالحواسيب) مقدمة في مؤتمر الامم المتحدة الحادي عشر لمنع الجريمة والعدالة الجنائية - بنكوك، 18 - 25 نيسان / إبريل 2005- صـ 14

(4) د.يونس عرب - صور الجرائم الإلكترونية واتجاهات تبويبها - مرجع سابق - صـ 8

تتميز بالطابع التقني والفني المعقد، والتي يصعب على أفراد الأجهزة الأمنية التعامل معها مثل جرائم الاعتداء بواسطة مجموعة حواسيب يزرع فيها برنامج يخضع لتحكم خارجي، ويطلق عليها (جرائم الاعتداء بواسطة شبكة البوتنت)[1]، حيث يمكن لأحد القراصنة التحكم في مجموعة من الحواسيب المـُخترقة الموجودة على إحدى شبكات البوتنت قد تصل إلى آلاف أو ملاين الأجهزة.[2]

د) صعوبة الوصول للدليل بفحص كميات هائلة من المعلومات.

ه) إحجام المجني عليهم في بعض الحالات عن الإبلاغ عن وقوع تلك الجرائم خشية من زعزعة ثقة عملائهم (مثل الجرائم التي تستهدف البنوك أو الشركات)[3] ، حيث أنه قد تكون الخسائر الكاملة أكبر من الخسائر الناجمة عن الهجوم الإلكتروني الذي تعرضوا له.

و) التحديات والصعوبات القانونية التي تعرقل عملية متابعة الجناة التي تنجم عن مشاكل الحدود والولايات القضائية وذلك نظراً لكون الجرائم المعلوماتية من طائفة الجرائم عابرة الحدود الوطنية.

---

(1) ورقة عمل بعنوان (التطورات الأخيرة في استخدام العلم والتكنولوجيا من جانب المجرمين والسلطات المختصة في مكافحة الجريمة، بما في ذلك الجرائم الحاسوبية) مقدمة في مؤتمر الأمم المتحدة الثاني عشر لمنع الجريمة والعدالة الجنائية – سلفادور، البرازيل، 12- 19 نيسان / أبريل 2010- صـ 2

(2) شبكة البوتنت: تنشأ شبكة البوتنت بزرع برنامج خبيث في الحاسوب المخترق والذي يسمى "بوت" ويتم توصيله أو إدراجه فيما بعد ضمن شبكة من الحواسيب المخترقة ويقدر عدد الأجهزة الموجودة بكل شبكة " بوتنت" حوالي 125000 جهاز. وتتيح هذه الشبكة للقراصنة بعد ذلك التحكم بها عن بعد لشن هجمات متفرقة لأغراض مختلفة مثل قطع الخدمة وسرقة معلومات مهمة، ونشر برامج خبيثة ، ويمكن للمخترق التحكم في مجموعة كبيرة من الحواسيب المخترقة الموجودة عى إحدى شبكات البوتنت والتي قد تصل إلى آلاف أو وملايين الأجهزة. كما أن أي شبكة بوتنت صغيرة قد تنقل قدرا هائلا من المعلومات والبيانات العشوائية كل ثانية – وهي كمية كفيلة بفصل خدمة الإنترنت عن معظم الشركات الكبرى وإعاقة عمليات مقدمي البنية التحتية من خلال التدخل في اتصالاتهم والبيانات المتدفقة والخدمات الأخرى التي تعتمد على الإنترنت. لكل ذلك تعد " شبكات البوتنت " أحد مصادر التهديد للبنية التحتية الحيوية نظراً لحجمها وقوتها وما تحتويه من برامج خبيثة. - راجع (مايكروسوفت ومخاطر شبكة البوتنت/البرامج الخبيثة للبنية التحتية الأساسية) – منشور على الموقع الإلكتروني الاتي:

http://www.amanak.org/ParentsandCare/PrintStuff/Arabic_Computing/docs/TwC-Elites-Botnets-One%20Pager-FINAL_Jun08.pdf

(3) د. أيمن عبدالله فكري – جرائم نظم المعلومات (دراسة مقارنة) – دار الجامعة الجديدة للنشر – الإسكندرية 2007 – صـ 94

3- تمتاز الجرائم المعلوماتية أيضاً من حيث حجم الخسائر الناجمة عنها والتي تفوق في معظم الأحيان تلك التي تترتب على الجرائم التقليدية فعلى سبيل المثال قام أحد مجرمي المعلومات وهو فلبيني الجنسية بصنع فيروس يسمى (أحبك) (I Love You) وقد انتشر هذا الفيروس في مختلف دول العالم عن طريق البريد الإلكتروني، وقدرت الخسائر الناجمة عن هذا الفيروس بحوالي (7) مليارات دولار [1].وقُدرت كلفة الإجرام المعلوماتي في العالم خلال عامي 2007 و2008، بنحو(8) مليارات دولار،وفيما يخص التجسس المعلوماتي على الشركات، فقد بلغت قيمة ما استولى عليه مرتكبي هذه الجرائم من ملكية فكرية لشركات تجارية (1 تريليون) دولار[2]. وكشفت إحصائية أجرتها المباحث الفيدرالية الأمريكية (FBI) في نهاية الثمانينات من أن جريمة الحاسب الآلي الواحدة تتكلف سنويا(600000) (ستمائة ألف) دولار أمريكي، في حين أن تكلفة جريمة السرقة الواحدة تحت الإكراه لا تزيد تكلفتها عن (3000) دولار سنويا.[3] كما يقدر مكتب التحقيقات الاتحادي الأمريكي خسائر الأعمال والمؤسسات التجارية الناتجة عن الجريمة المعلوماتية في الولايات المتحدة الأمريكية خلال عام 2005 بـ (67) بليون دولار أمريكي في السنة [4]. ويذكر أيضا أنه بحسب شركة سيمانتك الأمريكية لحماية الشبكة الإلكترونية فإن المعدل السنوي لكلفة الجرائم الإلكترونية حول العالم يبلغ 114مليار دولار. وقد أصدرت تقريرًا بعنوان «نورتون سايبركرايم 2011» وهو أكبر تقرير من نوعه حول كلفة الجرائم الإلكترونية، خلصت فيه إلى أن 431 مليون بالغ حول العالم كانوا ضحية للتهديدات الإلكترونية عام 2010

---

(1)جان فرنسوا هنروت - أهمية التعاون الدولي والتجربة البلجيكية في تبادل لمعلومات بين عناصر الشرطة والتعاون القضائي - برنامج تعزيز حكم القانون في بعض الدول العربية مشروع تحديث النيابات العامة - بحث مقدم بالندوة الاقليمية حول (الجرائم المتصلة بالكومبيوتر) في الفترة 19-20 نيسان / يونيو 2007 المملكة المغربية- صـ 95-97.

(2)http://www.interpol.int/ar

(3)د.محمد علي العرين ، مرجع سابق صـ18

(4)ورقة عمل بعنوان (التطورات الأخيرة في استخدام العلم والتكنولوجيا من جانب المجرمين والسلطات المختصة في مكافحة الجريمة، بما في ذلك الجرائم الحاسوبية) - مرجع سابق صـ 3

أي ما معدله مليون ضحية يوميًا و14 في الثانية. وقالت الشركة إن كلفة الجرائم الإلكترونية عام 2010 بلغت 388 مليار دولار وهي قيمة الخسائر المالية وخسارة الوقت، أي أنها تجاوزت قيمة السوق السوداء للماريجوانا والكوكايين والهيروين التي تبلغ 288 مليار دولا[1]. وتجدر الإشارة إلى أن هذه التقديرات قد لا تعكس حجم الخسائر الفعلي بسبب إحجام المجني عليهم في بعض الحالات عن الإبلاغ عن الجرائم التي يتعرضون لها خاصة الشركات والبنوك والمؤسسات المالية.

4- أما بالنسبة للدافع لارتكاب جرائم المعلوماتية فقد يكون أحياناً مجرد إظهار القدرات التقنية والمهارة في استخدام الحاسب هو السبب الوحيد لارتكابها[2] أو يكون الدافع بغرض اللهو والتسلية، أو رغبة مرتكبها في تحقيق انتصارات تقنية دون أن تتوافر لديه سوء نية في ارتكاب جريمة معينة كالسرقة أو الإتلاف أو التزوير وغيرها[3].

5- تمتاز الجريمة المعلوماتية بأنها جريمة عابرة الحدود لا تحدها حدود الدول، فهي متمردة على عنصر المكان والنطاق الجغرافي[4] ، حيث تدخل في طائفة الجرائم عبر الوطنية، ويرجع ذلك إلى البيئة الإلكترونية التي تقع فيها تلك الجرائم والتي تقوم على الربط الإلكتروني بين الحواسيب سواء داخل الدولة الواحدة أو بين عدة دول بواسطة شبكات الكترونية مثل الانترنت والتي صممت في الأصل لتسهيل عملية نقل المعلومات والاتصالات، فأضحت تستخدم كوسيلة لارتكاب الجرائم، فقد ترتكب جريمة بواسطة الحاسب الآلي عن طريق الشبكات الدولية (الإنترنت) وتتحقق نتيجتها الإجرامية في دولة أخرى من العالم مروراً بمزود خدمة أو قنوات اتصال في إقليم دولة ثالثة. ويترتب على البعد عبر الوطني للجريمة المعلوماتية عدة إشكاليات مشابهة لتلك المرتبطة بالجرائم ذات الطابع عبر الوطنية أهمها، اصطدام إجراءات التحقيق

---

(1) جريدة الراية الاقتصادية القطرية الخميس 29 ربيع الآخر 1433 هـ - 22 مارس 2012 م - العدد (10911) صـ 8

(2) د.نائلة عادل محمد فريد قورة – جرائم الحاسب الاقتصادية (دراسة نظرية وتطبيقية) – دار النهضة العربية – القاهرة 2004/2003 - صـ45

(3) د. محمد على العرين ، مرجع سابق صـ63 - 65

(4) د. أيمن عبدالله فكري – مرجع سابق – صـ92

وضبط المتهمين وملاحقتهم بمبدأ السيادة الوطنية للدولة وخاصة في الجرائم التي تتطلب اتخاذ إجراء من إجراءات التحقيق في إقليم دولة أجنبية، وكذلك إشكالية الاختصاص القضائي وإشكالية تحديد القانون واجب التطبيق. كما أنه من جهة آخرى تشكل الإجراءات الرسمية المعقدة والتي تستغرق وقتا ليس بالقصير في حالات المساعدة القانونية أو القضائية بين الدول، والتي تتعارض مع طبيعة الجرائم المعلوماتية التي تتطلب سرعة في التحقيقات[1] حيث أن جزءاً كبيراً من الأدلة في الجرائم المعلوماتية كما سبق الإشارة غير ملموس ويزول بسرعة، وهو ما يتطلب أن تكون إجراءات التحقيق وجمع الأدلة بصورة سريعة وآنية.

ونخلص مما تقدم أن الجريمة الإلكترونية ليست جريمة تقليدية في ثوب جديد، وإنما هي بحق نوع مستحدث من الجرائم الذي يتطلب مكافحتها جهداً تشريعيا وتعاوناً دوليا فاعلين.

---

(1) ورقة عمل بعنوان (التطورات الأخيرة في استخدام العم والتكنولوجيا من جانب المجرمين والسلطات المختصة في مكافحة الجريمة، بما في ذلك الجرائم الحاسوبية) - مرجع سابق صـ 5

المطلب الثالث

المجرم المعلوماتي

المجرم المعلوماتي هو مصدر الخطر في جرائم المعلوماتية ، وهو من يتعين مواجهته والتصدي له ووقف عدوانه وتهديداته للنظم المعلوماتية والمعلومات والبيانات الإلكترونية، وإن فهم صفاته الشخصية ودوافعه، وماهية تفكيره، وأسلوبه في ارتكاب جريمته ووسائله المختلفة، يُعد أمراً ضرورياً ولازماً لإيجاد أفضل الوسائل وأكثرها فاعليه لمكافحة إجرامه وعدوانه وبالتالي مكافحة الجريمة المعلوماتية بالمفهوم الواسع، لذا سنتناول في هذا المطلب السمات الشخصية للمجرم المعلوماتي، وفئاته، ودوافعه لارتكاب الجريمة ، وسنتناول وسائله في ارتكاب الجرائم موضوع البحث عند تناول كل جريمة على حدة.

الفرع الأول

سمات المجرم المعلوماتي

تختلف الجرائم وتتنوع من حيث طبيعتها ومحلها وأدواتها وحتى مرتكبيها، إذ تتطلب بعض الجرائم توافر سمات أو خصائص معينة في مرتكبيها، مثل البنية الجسمانية القوية والقوة العضلية، أو الذكاء والدهاء. حيث يذهب البعض[1] إلى هناك أنواعا من الجرائم يرتبط ارتكابها والإقبال عليها أو العزوف عنها بدرجة الذكاء التي يتمتع بها كل مجرم، وتبعا لذلك فقد ذهبوا إلى تقسيم الجرائم إلى نوعين:

- **النوع الأول:** جرائم الذكاء وهي التي يقبل على ارتكابها المجرمون الأكثر ذكاء لما تتطلبه من القدرة على اختيار أنسب الظروف المحيطة بالجريمة وما تتطلبه من مهارة وخداع وطرق احتيالية مثل جرائم الاحتيال والتزوير والجرائم الاقتصادية.

---

(1) د. فوزية عبدالستار - مبادئ علم الاجرام وعلم العقاب - دار المطبوعات الجامعية - الإسكندرية - 2007 صـ126

- **النوع الثاني:** جرائم الغباء وهي التي يقبل عليها ضعاف العقول، والتي لا تتطلب مجهوداً ذهنياً عالياً. مثل جرائم التسول والاعتداء.

مع الإشارة إلى أن هذا لا يعني اقتصار جرائم الذكاء على الأذكياء وجرائم الغباء على ضعاف العقول، فكل من هذه الجرائم قد تقع من أي مجرم مهما كانت قدراته العقلية.

ويمكن تصنيف الجرائم المعلوماتية ضمن طائفة جرائم الذكاء، فهي جرائم تشكل التقنية الحديثة أهم عناصرها من حيث كونها الوسيلة المستخدمة في الجريمة أو أنها تشكل محل الاعتداء في تلك الجرائم، فضلاً عما يتطلبه ارتكاب تلك الجرائم من مهارة في استخدام التقنية الحديثة والبحث عن الثغرات في النظم المعلوماتية واكتشاف الطرق المختلفة للتحايل عليها، واختراق تلك النظم والخروج منها بعد محو آثار اعتدائهم بكل مهارة، وهو كله يتطلب توافر قدر معقول من الذكاء إضافة للعلم والمعرفة والمهارة لدى مرتكبيها. فالمجرم المعلوماتي هو إنسان ذكي، يتمتع بقدر من الاحترافية في استخدام الحاسب الآلي والشبكات الإلكترونية، على نحو يمكنه من اختراق النظم المعلوماتية وسرقة المعلومات أو إتلافها أو تزويرها، وارتكاب غيرها من الجرائم المعلوماتية الآخرى. وللتعرف أكثر على شخصية المجرم المعلوماتي **نستعرض أهم خصائص شخصيته فيما يأتي:**

1- أنه في الغالب مجرم متخصص يتمتع بالقدرة الفائقة والمهارة التقنية العالية، ويستغل قدراته هذه في اختراق الشبكات والنظم المعلوماتية وكسر كلمات المرور والشفرات السرية، وسرقة المعلومات والبيانات والاحتيال الإلكتروني، وكذلك الاعتداء على حقوق الملكية الفكرية مقابل المال.

2- أنه مجرم غالبا ما يعود إلى ارتكاب هذه الجريمة حيث كثيراً ما يعول على مهاراته في استخدام الحاسب الآلي والتحكم في نظم الشبكات وغيرها للدخول غير المصرح به مرات ومرات، بالإضافة إلى أن صعوبة ضبط وتعقب الجناة في هذا النوع من الجرائم في حالات عدة إما لصعوبات تقنية أو قانونية سبق وأن

أشرنا إليها، وإما لإحجام بعض المجني عليهم عن الإبلاغ عن الجرائم التي تعرضوا لها مثل الشركات والبنوك ومؤسسات المال خوفا على سمعتهم وثقة العملاء، كل ذلك يشكل حافزا لتكرار المجرم المعلوماتي لجريمته.

3- أنه مجرم ذكي يمتلك المهارات التي تؤهله لتعديل وتطوير الأنظمة الأمنية على النحو الذي يوفر له الحماية من ملاحقة الأجهزة الأمنية وتتبع أعماله الإجرامية.[1]وذلك من خلال إخفاء شخصيته، وإخفاء المكان (الدولة أو المدينة) التي يمارس منها نشاطه.حيث أنه غالبا ما يقوم المخترق بالتحكم بجهاز الضحية، ويقوم باستخدامه للتحكم بأنظمة أجهزة آخرى، وذلك بهدف إخفاء مكانه الأساسي والتخفي بجهاز الضحية. ويعمل المجرم المعلوماتي وخاصة في جرائم الاختراق على تعزيز وجوده داخل النظام المعلوماتي المخترق وذلك بقيامه بإحداث ثغرات إضافية في النظام المعلوماتي بحيث يمكنه العودة من خلالها في المستقبل في حالة ما إذا اكتشفت الثغرة التي نفذا منها في أول مرة.

4- من أبرز سمات مجرمي المعلومات التعاونية؛ حيث يميلون إلى العمل سوياً، وذلك من خلال قيامهم بإنشاء صفحات خاصة بهم في الانترنت[2]، بل

(1) د. فؤاد جمال - الجريمة الإلكترونية - جريدة الأهرام العربي - العدد 566 بتاريخ 2008/1/26 منشور على الموقع الإلكتروني:

http://arabi ahram org.eg/arabi/Ahram/2008/1/26/INVS6.HTM

(2) مثال الموقع الإلكتروني الخاص بالهاكرز ، http://www.defcon org/html/defcon-19/dc-19-index.html ، فضلا عن أنهم يعقدون مؤتمرهم السنوي في لاس فيغاس باسم ديفكون DefCon ، وهو تجمع يلتقي فيه هؤلاء لاستعراض مهاراتهم والتباهي بالمقالب التي يوقعون بها الآخرين باصطياد مواقعهم وبياناتهم وكمبيوتراتهم والتحكم بها عبر الإنترنت، وكان اخر مؤتمر لهم في الفتره من 4 – 7 اغسطس 2011

- وفي أغسطس 2011نظم قراصنة الكمبيوتر مهرجاناً خاصاً بهم في مدينة فونوفورت الألمانية بمشاركة حوالي ثلاثة آلاف وخمسمائة شخص من حوالي خمس وأربعين دولة. ويهدف هذا المهرجان إلى إتاحة الفرصة للمشاركين فيه من قراصنة الكمبيوتر التعرف على آخر الوسائل والأجهزة الإلكترونية الحديثة المستخدمة في هذا المجال وتبادل الخبرات فيما بينهم. وقد ذكرت إحدى المشاركات في هذا المهرجان أن " هذا ليس تجمعاً للمجرمين ولا يحمل نية سيئة، معظم المشاركين هنا جاؤوا للتعرف على أحدث أنواع التكنولوجيا و كيف تعمل، و أين هي حدود التكنولوجيا."

وقد تمكن القائمون من تأمين اتصال الإنترنت لحوالي خمسة آلاف كمبيوتر تعمل في المهرجان و تحمل في جعبتها كل ما هو جديد في عالم القرصنة. المرجع:

http://arabic.euronews.net/2011/08/14/computers-under-canvas-at-hackers-summer-camp

ويعقدون مؤتمرات خاصة بهم، فإذا نجح أحدهم في اختراق شبكة أو نظام ما فإن هذه الشبكة أو هذا النظام يكون في حكم المخترق من جميع المهاجمين[1].

ومن جانب آخر يوجز البعض[2] الخصائص التي تميز المجرم المعلوماتي في المهارة- المعرفة- الوسيلة - السلطة- والباعث[3]، وبيان المقصود بتلك الخصائص كالآتي:

1- **المهارة**؛ يستلزم تنفيذ الجريمة المعلوماتية تمتع الجاني بقدر كافي من المهارة في استخدام الوسائل التقنية الحديثة كالحاسب الآلي مثلاً، و التي يكتسبها إما من خلال الدراسة أو الخبرة العملية في مجال تكنولوجيا المعلومات، بحيث يكون بمقدوره اختراق الأنظمة المعلوماتية وبرامج الحماية وفك الشفرات السرية الخاصة بها وبالتالي الحصول على المعلومات والبيانات المخزنة داخل تلك الأنظمة.

2- **المعرفة**؛ تعني تعرف الجاني على الظروف المحيطة بجريمته بحيث لا يفاجأ بأشياء غير متوقعة، إذ يقوم المجرم المعلوماتي بتكوين تصور كامل لجريمته وذلك من خلال تطبيق جريمته على أنظمة معلوماتية مشابهه لتلك التي يستهدفها وذلك قبل تنفيذ الجريمة.

3- **الوسيلة**؛ يقصد بها الإمكانيات اللازمة التي يحتاج إليها الجاني لتنفيذ جريمته فبالنسبة للجريمة المعلوماتية فإن الوسائل اللازمة لاختراق أنظمة

---

(1) حسن طاهر داود – أمن شبكات المعلومات- معهد الادارة العامة ، مركز البحوث، المملكة العربية السعودية 2004 – صـ104

(2) يذهب الأستاذ Parker إلى أنه وإن كان يمتاز ببعض السمات الخاصة إلا أنه في نهاية المطاف لا يخرج عن كونه مجرماً مرتكباً لفعل محرم مما يتعين معه معاقبته على مقترفه من أفعال مجرمة، ويضيف أن كل ما في الأمر أنه ينتمي إلى نوع خاص من المجرمين تتشابه من حيث خصائصها الإجرامية مع جرائم ذوي الياقات البيضاء، فالمجرم المعلوماتي في أغلب الأحيان ينتمي إلى وسط اجتماعي متميز كما وإنه يكون على درجة من العلم والمعرفة وهو ما يميز بشكل عام ذوي الياقات ابيضاء، وإن كان كما يرى أنه ليس من الضروري أن ينتمي المجرم المعلوماتي إلى مهنة معينة يرتكب من خلالها جريمته كما هو الشأن بالنسبة لذوي الياقات البيضاء. كما يتفق المجرم المعلوماتي مع ذوي الياقات البيضاء في أن كل منهما يحاول إيجاد مبرر لجريمته ولا ينظر إلى سلوكه على أنه جريمة أو فعل منافي للقيم والأخلاق. أشارت إليه د.نائلة عادل محمد فريد قورة – مرجع سابق صـ51- 52

(3) المرجع نفسه صـ 52 -53-54

الحاسبات الآلية غالبا ما تمتاز بالبساطة النسبية وسهولة الحصول عليها فالمجرم المعلوماتي يمتاز بقدرته على الحصول على ما يحتاجه أو ابتكار أساليب تقلل من الوسائل المتطلبة لتنفيذ نشاطه الإجرامي.

4- **السلطة**: تعني الحقوق والمزايا التي يتمتع بها الجاني بالنسبة للجرائم المعلوماتية والتي تمكنه من تنفيذ جريمته. حيث إن كثيرا ما يكون لمجرمي المعلومات سلطة مباشرة أو غير مباشرة على المعلومات محل الجريمة. وقد تتمثل هذه السلطة في الشفرة الخاصة بالدخول إلى نظام المعلومات والتي يتمكن من خلالها المجرم من فتح الملفات ونسخها أو تعديلها أو نقلها. كما قد تتمثل تلك السلطة في الحق في استعمال الحاسب الآلي أو الدخول إلى الأماكن التي تضم أنظمة الحاسبات الآلية. كما أنه قد تكون تلك السلطة مستمدة من الحصول على شفرة الدخول الخاصة بشخص آخر واستخدامها للدخول إلى نظام المعلومات.

5- **الباعث أو الدافع لارتكاب الجريمة**: فإنه في كثير من الأحيان لا يختلف عن الدافع لارتكاب الجرائم التقليدية الآخرى من رغبة في الكسب المادي السريع بطريق غير مشروع ، ثم يلي ذلك مجرد الرغبة في قهر النظم المعلوماتية وتخطي حواجز الحماية، أو قد يكون الرغبة في الانتقام من رب العمل أو أحد الزملاء. وأيا كان الباعث فإن المجرم المعلوماتي في كثير من الأحيان لا يرى فيما يقوم به من حرج أو ما يشكل جريمة أو انتهاكا للأخلاقيات وخاصة في الحالات التي يكون الدافع فيها مجرد تحدي النظم الإلكترونية أو المعلوماتية.

وعلى الرغم من حصافة الرأي المتقدم، وعلى الأرجح فأن المجرم المعلوماتي قد يتسم بسمات المهارة والوسيلة والباعث والذكاء دون سمتي المعرفة والسلطة **وتبرير ذلك كالآتي**:

- **فالمعرفة**: بمعنى أن يكوّن لدى المجرم المعلوماتي تصوراً كاملاً عن جريمته من خلال تطبيق جريمته على أنظمة معلوماتية مشابهه لتلك التي يستهدفها قبل تنفيذ الجريمة، فهي سمة تتوفر لدى جميع المجرمين وليست سمة

خاصة بالمجرم المعلوماتي. فالمجرم في جرائم السرقة والاحتيال وحتى جرائم القتل يقوم بتكوين تصور كامل لجريمته ويتلقى التدريب المناسب لضمان نجاحه في تنفيذ جريمته.

- **أما بالنسبة للسلطة:** فكثير من الجرائم المعلوماتية ترتكب من قبل أشخاص لا تربطهم علاقة بالمجني عليه سواء كان فرد أو مؤسسة، وليس له أي سلطة مباشرة أو غير مباشرة على المعلومات محل الجريمة مثال ذلك، جرائم الالتقاط أو الاعتراض غير القانوني للبيانات، والتزوير المعلوماتي، والاختراق.

وتجدر الإشارة إلى إن الإجرام المعلوماتي لا يقتصر على الأشخاص الطبيعيين فحسب، بل يمتد ليشمل الأشخاص المعنوية من شركات، ومؤسسات، بل وحتى دول، وهو ما أكدت عليه العديد من التشريعات والاتفاقيات الخاصة بالجرائم المعلوماتية ومنها اتفاقية مجلس الاتحاد الأوروبي - بودابست لسنة 2001 المتعلقة بالجريمة الإلكترونية حيث تنص المادة (12) منها على أنه (1- يجب على كل طرف أن يتخذ الإجراءات التشريعية، وأية إجراءات آخرى يرى أنها ضرورية من أجل اعتبار الأشخاص المعنوية مسئولة عن الجرائم المشار إليها في الاتفاقية الحالية، إذا ارتكبت لمصلحتها، عن طريق أي شخص طبيعي، يتصرف بشكل فردي، أو بوصفه عضوا في مؤسسة الشخص المعنوي، ويمارس سلطة القيادة في داخله بناء على القواعد التالية:

أ) سلطة تمثيل الشخص المعنوي

ب) سلطة اتخاذ القرارات باسم الشخص المعنوي

ج) سلطة ممارسة الضبط داخل الشخص المعنوي

2- بالإضافة إلى الحالات التي سبق النص عليها في الفقرة (1)، فأنه يجب على كل طرف أن يتخذ الإجراءات الضرورية من أجل التأكد من أن الشخص المعنوي يمكن أن يكون مسئولا إذا تخلفت المراقبة أو الضبط من جانب شخص طبيعي مشار إليه في الفقرة (1) قد جعل من الممكن ارتكاب الجرائم المشار إليها

في الفقرة (1) لحساب الشخص المعنوي عن طريق شخص طبيعي يتصرف تحت سلطته.

3- تبعا للمبادئ القانونية للطرف، فإن مسئولية الشخص المعنوي، يمكن أن تكون جنائية، أو مدنية ، أو إدارية.

4-هذه المسئولية يجب أن تكون دون أضرار بالمسئولية الجنائية للأشخاص الطبيعيين الذين ارتكبوا الجريمة.)[1]

---

(1) د.هلالي عبداللاه أحمد - الجوانب الموضوعية والإجرائية لجرائم المعلوماتية على ضوء اتفاقية بودابست الموقعة في 23 نوفمبر 2001 - دار النهضة العربية - القاهرة -الطبعة الأولى 2003 - صـ 148-150

الفرع الثاني

فئات المجرم المعلوماتي

يمكن تقسيم فئات مجرمي المعلوماتية إلى عدة فئات وذلك تبعاً لأهدافهم ودوافعهم لارتكاب جرائمهم، وبيان ذلك على النحو الأتي:

1- الباحثون عن المغامرة والتسلية: يتضح من تسمية هذه الفئة، أن ما يأتونه من أفعال تشكل جرائم معلوماتية، مثل جرائم الاختراق، والدخول غير المشروع إلى النظام المعلوماتي، لا يكون بدافع إجرامي أو بنية الأضرار بالغير، وإنما يكون بدافع التسلية والمغامرة. ويشكل الشباب وصغار السن غالبية هذه الفئة،حيث يبحثون عن التسلية والمغامرة والتنافس واستعراض قدراتهم ومهاراتهم أمام أقرانهم في استخدام الحاسب الآلي والقدرة على اختراق الحاسبات الآخرى.

ورغم أن دوافع أفراد هذه الفئة ليست إجرامية، إلا أنه يتعين أخذ الحذر منهم، وعدم غض الطرف عنهم، إذ إن اعتياد هؤلاء الشباب على إتيان تلك الأفعال وتماديهم فيها قد يشكل خطوة أولى على طريق الإجرام واحتراف الجريمة المعلوماتية، فضلا عن أنه من الممكن أن يسقطوا فريسة في شراك العصابات والمنظمات الإجرامية لضمهم إليها لاستغلال مواهبهم تلك لارتكاب الجرائم [1] مستغلين فيهم حداثة سنهم وقلة خبرتهم.

وإذا كان المنتمون لهذه الفئة يأتون أفعالهم من باب الفضول والمغامرة، دون نية الأضرار العمدي بالغير،إلا أنه في الغالب ما يترتب على أفعالهم أضرار بالأنظمة المعلوماتية، والأضرار بمصالح المجني عليهم [2]،فضلا عما قد يترتب

(1) د. محمد سامي الشوا - ثورة المعلومات وانعكاساتها على قانون العقوبات - دار النهضة العربية - القاهرة - الطبعة الثانية، صـ 41

(2) تمكن صبي كندي في الخامسة عشرة من عمره عام 2000 من السيطرة على عدد من أجهزة الحاسب الآلي واستخدامها في شن هجمات متفرقة ضد شركتي (Yahoo , Amazon.com) ومواقع أخرى في مجال التجارة الإلكترونية بهدف الحرمان من الخدمات، حيث قام بتخفيض سرعة النفاذ إلى هذه المواقع أو تقييد النفاذ إليها، وقد تكبدت هذه الشركات نتيجة لتلك الهجمات خسائر تقدر بمئات الملايين من الدولارات بسبب ضياع الصفقات وعدم الاستفادة من السوق، بالإضافة إلى تكاليف تحسين أمنتلك المواقع المرجع - ورقة عمل بعنوان (تدابير لمكافحة الجرائم المتصلة بالحواسيب) مقدمة في مؤتمر الأمم المتحدة الحادي عشر لمنع الجريمة والعدالة الجنائية- مرجع سابق صـ 7

على هجماتهم تلك خلق ثغرات فيها تمكن غيرهم من المهاجمين ذوي النوايا الإجرامية،مما يعرض المعلومات والأسرار المخزنة في الحاسب الآلي، أو المنقولة بواسطة الشبكات الإلكترونية لخطر الإفشاء أو السرقة أو الإتلاف أو غير ذلك من أخطار.

2- **المخربون**: التخريب هو هدف هذه الفئة من مجرمي المعلومات، فهم يعمدون إلى إتلاف ومسح البيانات والمعلومات المخزنة في الحاسبات الآلية أو المنقولة عبر الشبكات، ويعد الرغبة في الانتقام أحد أهم دوافع تلك الفئة سواء انتقام العامل من رب العمل نتيجة لعدم التقدير أو في حال تسريحه من العمل ، أو الانتقام بدافع ديني[1]، أو سياسي[2]،أو انتقاما من الدولة اعتراض على أداء الحكومة أو سوء الأوضاع الاقتصادية [3].

---

(1) قررت مجموعة من الشباب السعودي استغلال قدراتهم في التعامل مع الإنترنت للدفاع عن الرسول الكريم والتصدي للرسوم الكاريكاتيرية المسيئة له على طريقتهم الخاصة فتسللوا إلى هذه المواقع ودمروا أغلبها حيث قام شاب لم يتجاوز عمره الـ21 عاما بتكوين منظمة مع أصدقائه أطلق عليها منظمة "قراصنة حائل" هدفهم محاربة كل المواقع المعادية للإسلام ورسوله، والمواقع التي تنشر الدعارة وتسئ لأخلاق شباب الأمة العربية.وقد قام هذا الشاب بالتعاون مع أصدقائه في اختراق وتدمير موقع الصحيفة الدانمركية "يولاندر بوسطن" أولى الصحف الغربية التي نشرت الرسوم المسيئة لرسولنا عليه الصلاة والسلام.

وفي ذات السياق استطاع هاكر سعودي من تدمير نحو (71) موقعا دانماركيا أساءت للرسول صلى الله عليه وسلم،مؤكدا على ان الدافع الحقيقي لتدمير تلك المواقع هو الغيرة على الدين الإسلامي والمسلمين. - راجع

http://en-gb.facebook.com/topic.php?uid=117618218275528&topic=156

(2) تعرضت إسرائيل لهجمات الكترونية كبيرة تم على إثرها تدمير أكثر من (700) موقع انتقاما للدمار الذي لحق بالمرافق البنانية (حسب صحيفة يدعوت أحرنوت التي حذرت مرارا مما أسمته حملات الجهاد الإلكتروني E-Jehad) وقد أتت أكبر الهجمات العربية من المغرب - وتحديدا من شلة مراهقين تدعى "نادي الشياطين" - في حين أتت أكبر الهجمات الإسلامية من تركيا وإيران بعد ثلاثة أيام فقط من بدء الحملة العسكرية.وجدير بالذكر أن البداية الحقيقية لهجمات الهكرز - ضد إسرائيل - بدأت بعد مقتل الطفل محمد الدرة حيث تم تدمير مواقع بعض الوزارات ووضع صورة "الدرة" على صفحتها الأولى . ومع بدء قصف غزة - الذي سبق الهجوم على لبنان - تعرضت وزارة الدفاع الإسرائيلية لـ 17محاولة اختراق في حين تم تدمير عدد كبير من مواقع الشركات والمؤسسات الحكومية المهمة. (مقال بعنوان (كتيبة الفيروسات وجمعية الهكرز السعودي) جريدة الرياض - العدد 14042 - الاثنين 13 ذي القعدة 1427هـ -4 ديسمبر 2006م

http://www.alriyadh.com/2006/12/04/article206367.print

(3)دخل أحد قراصنة الإنترنت للموقع الرسمي لرئاسة الجمهورية البلغارية على شبكة الإنترنت، وقام بمحو كل محتوياته قبل أن يترك رسالة على الموقع يذكر فيها إن دافعه وراء هذا العمل هو التعبير عن السخط من الحالة المزرية لحياة والديه، في الوقت الذي لا يجد فيه عملا، في حين اضطر العديد من أصدقائه للهجرة لتحسين مستقبلهم في الخارج. راجع

http://www.aljazeera.net/news/archive/archive?ArchiveId=2187

3- الساعون إلى الربح: تستهدف هذه الفئة من هجماتها السطو على المعلومات التي يمكن تحويلها إلى أموال[1] سواء بعد بيعها أو استخدامها، مثال ذلك استهداف الحسابات البنكية، الأرقام السرية لبطاقات الائتمان، أو الحصول على الأسرار التجارية الخاصة بمنتج معين أوالتصاميم الصناعية الخاصة بإحدى الشركات، وفي الحالة الأخيرة نكون أمام فرضين: الأول؛ قيام الجاني باستخدام تلك الأسرار أو التصاميم في إعادة إنتاج أو تصنيع المنتج وجني الربح من وراء ذلك، والفرض الثاني؛ قيام الجاني ببيع ما تحصل عليه من أسرار أو رسومات أو تصاميم إلى شركات آخرى منافسة للشركة المجني عليها.

4- الجواسيس : عرّفت المادة 29[2] من اتفاقية لاهاي للعام 1907 الخاصة باحترام قوانين وأعراف الحرب البرية الجاسوس، بأنه ذلك الذي يقوم بأفعال وممارسات في الخفاء أو عن طريق الخداع أو التنكر بهدف البحث أو الحصول على معلومات من دولة بغرض نقلها أو إيصالها إلى دولة آخرى عدوة.

وعرفت المادة 46[3] من البروتوكول الإضافي الأول الملحق باتفاقيات

---

(1) قام موظف صيني قبل استقالته من الشركة التي يعمل بها بالاستيلاء على برمجيات ورموز أساسية تقدر بمبلغ (950 ألف دولار) يمكن ان تؤدي عند انتاجها إلى مليارات الدولارات، وقد أدى ذلك إلى إعلان الشركة إفلاسها وتسريح موظفيها. - د. ذياب البداينة - الأمن وحرب المعلومات - عمان - الاردن - دار الشروق 2002 - صـ 255

(2) تنص المادة (29) من اتفاقية لاهاي للعام 1907 الخاصة باحترام قوانين وأعراف الحرب البرية على انه (لا يعد الشخص جاسوساً إلا إذا قام بجمع معلومات أو حاول ذلك في منطقة العمليات التابعة لطرف في النزاع، عن طريق عمل من أعمال الزيف أو تعمد التخفي، بنية تبليغها للعدو.

ومن ثم لا يعد جواسيس أفراد القوات المسلحة الذين يخترقون منطقة عمليات جيش العدو، بنية جمع المعلومات، ما لم يرتكب ذلك عن طريق التخفي عنوة. كذلك لا يعد جواسيس: العسكريون وغير العسكريين الذين يعملون بصورة عنية، والذين يكتفون بنقل المراسلات الموجهة إما إلى جيشهم أو إلى جيش العدو ...) .

(3) تنص المادة 46 من البروتوكول الإضافي الأول الملحق باتفاقيات جنيف 1949 والمتعلق بحماية ضحايا المنازعات الدولية المسلحة على أنه (...2- لا يعد مقارفاً للتجسس فرد القوات المسلحة لطرف في النزاع الذي يقوم بجمع أو يحاول جمع معلومات لصالح ذلك الطرف في إقيم يسيطر عليه الخصم إذا ارتدى زي قواته المسلحة أثناء أدائه لهذا العمل.

3-لا يعد مقارفاً لتجسس فرد القوات المسلحة لطرف في النزاع الذي يقيم في إقيم يحتله الخصم والذي يقوم لصالح الخصم الذي يتبعه بجمع أو محاولة جمع معومات ذات قيمة عسكرية داخل ذلك الإقليم، ما لم يرتكب ذلك عن طريق عمل من أعمال الزيف أو تعمد التخفي....)

جنيف 1949 والمتعلق بحماية ضحايا المنازعات الدولية المسلحة الجاسوس بأنه ذلك الذي يجمع أو يحاول جمع معلومات ذات قيمة عسكرية، في الخفاء أو باستعمال الغش والخداع.

إذا فالتجسس بمفهوم عام هو العمل في الخفاء أو تحت إي صفة كاذبة وباستخدام التنكر والخداع للحصول على معلومات عن جهة معينة (دولة ، شركة، أو أفراد عاديين) بهدف نقلها إلى جهة آخرى تسعى إلى الحصول على تلك المعلومات.

ولقد أدى تطور أساليب التخفي والخداع الإلكتروني بتصميم برامج خصيصا لهذا الغرض إلى تيسير عمليات التجسس، وسهلت على الجاسوس المعلوماتي تحركاته في الفضاء الإلكتروني، ولا تقف هذه الأساليب الخداعية عند حد معين بل هي في تطور مستمر. والتجسس المعلوماتي قد يرتكب من قبل بعض الأفراد الطبيعيين، أو من قبل الأشخاص المعنوية دول أو شركات ومؤسسات[1].

وتكمن خطورة التجسس المعلوماتي في سرقة المعلومات بمختلف أنواعها، وما يترتب على ذلك من استثمار غير شرعي لجهود الآخرين من أبحاث وبراءات اختراع وغيرها والتربح منها، على فرض تعلق المعلومات المسروقة بأبحاث علمية أو معلومات تجارية أو اقتصادية، فضلا عما يشكله من تهديد لأمن الدول إذا ما كان موضوع تلك المعلومات عسكريا أو سياسيا. وأكثر ما تخشاه الدول أنه قد يترتب على التجسس المعلوماتي النقل غير قانوني للتقنية وخاصة في المجال العسكري ومجال صناعة الأسلحة إلى دول معادية أو جماعات إرهابية تستخدم ما توصلت إليه من معلومات ومعرفة تقنية في تطوير إمكاناتها

---

(1) لقد حاولت شركتي هيتاش وميتسوبيشي اليابانيتين، التجسس على شركة الحاسبات الآلية (IBM) الأمريكية، كما حاولت أجهزة الاستخبارات الفرنسية التجسس على ذات الشركة الأمريكية ولكن لمصلحة الشركة الفرنسية المنتجة للحاسبات الآلية (BUII) د. عمر أبو الفتوح عبدالعظيم الحمامي – الحماية الجنائية للمعلومات المسجلة إلكترونيا – دار النهضة العربية - القاهرة 2010 - صـ105

التقنية أو التسليحية مما يشكل تهديدا للجهة المعتدى عليها أو المجتمع الدولي ككل[1]، وفي هذا السياق فقد تمكنت مجموعة من قراصنة الكمبيوتر في عام 2009 من اختراق برامج أكثر مشاريع وزارة الدفاع الأميركية (البنتاغون) تكلفة، حيث تمكن المتطفلون من الدخول إلى برنامج مشروع الطائرة النفاثة المقاتلة المعروفة بـ (إف 35 لايتننغ 2) بتكلفة ثلاثمائة مليار دولار- كما تمكنوا من نسخ بيانات تتعلق بالتصميم والأنظمة الإلكترونية، الأمر الذي يسهل اتخاذ إجراءات دفاعية ضد هذه الطائرة. ويرجح البعض أن يكون مصدر هذه الهجمات من الصين، رغم صعوبة تحديد المصدر الحقيقي بسبب سهولة التخفي وراء هويات مقنعة[2].

ويعد التجسس المعلوماتي من أخطر صور الجرائم المعلوماتية وأكثرها تهديداً للنظم المعلوماتية، حيث ذكر مدير نظم الحلول العالمية بإحدى شركات التأمين الشهيرة أن أخطر تهديد يواجه شبكة الإنترنت هو البرامج التجسسية وليست الفيروسات. فقراصنة الانترنت كانوا يهدفون فيما مضى إلى تدمير الحاسبات عن

(1) أعلن لويس ريجل مساعد مدير المباحث الفيدرالية الأمريكية والمسئول عن قسم الجرائم الإلكترونية علي الإنترنت أن تنظم القاعدة لا يملك الإمكانيات التقنية التي تجعله يشكل تهديدا خطيرا علي شبكة الإنترنت العالمية. رغم ذلك فإنه يقول أن هناك مجموعة من المنظمات الإرهابية تقوم بشكل دوري بمحاولة اختراق شبكات الحاسبات في محطات توليد الطاقة الكهربائية الكبرى والمطارات العالمية وغيرها من مكونات البنية الأساسية العالمية الحساسة.الغريب أن ما تخشاه المباحث الفيدرالية الأمريكية هي الحكومات الأخرى وليست المنظمات الإرهابية فقط. فأحد المحققين الأمريكيين يقول أن هناك الآلاف من المواقع الصينية التي تحاول الدخول علي حاسبات البنتاجون والحصول علي بيانات بطريقة غير مشروعة وباستخدام برامج تجسسية متقدمة. تقوم جهات التأمين الأمريكية بعمليات هجوم معاكسة لكي تتعرف علي هوية القراصنة الذين يحاولون احتراق المواقع الأمريكية والحصول علي بيانات سرية من علي الحاسبات الإلكترونية المتصلة بالشبكة. يقول المحقق الأمريكي إن هناك محاولات لسرقة المعلومات من علي شبكة الإنترنت -لا يستطيع القراصنة التقليدين القيام بها وهي عمليات في غاية التنظيم والكفاءة ولا يستطيع القيام بها إلا مؤسسات عسكرية أجنبية يقول الخبراء إن القراصنة ربما لا يستطيعون الحصول علي بيانات حساسة من مواقع البنتاجون علي شبكة الإنترنت بسبب كفاءة نظم التأمين بها ولكن المقاولين الذين يتعاملون مع الجيش الأمريكي قد لا تكون حاسباتهم ومواقعهم علي شبكة الإنترنت تحظي بنفس الدرجة العالية من التأمين.- جريدة الأهرام، الثلاثاء الموافق 7 مارس 2006 العدد 43555 -

http://ait.ahram.org.eg/ait/Ahram/2006/3/7/Ait43555_4m.jpg

(2)http://www.aljazeera.net/NR/exeres/265131A2-AF2E-478F-9CB4-8301B1E039B8.htm

طريق تطوير الفيروسات المدمرة، إلا أنهم لاحظوا أنهم كانوا يضيعون طاقاتهم بدون مقابل، لذلك فقد ارتأوا استغلال خبراتهم التقنية العالية والساعات الطويلة التي يقضونها أمام حاسباتهم. حيث قام هؤلاء القراصنة بتطوير برامج تجسسية تستطيع الوصول إلي أرقام بطاقات الائتمان التي تستخدم في الشراء عبر شبكة الإنترنت وسرقة أرقام حسابات عملاء البنوك وذلك للقيام بعمليات السرقة الإلكترونية. كما قام هؤلاء القراصنة بتشكيل عصابات إلكترونية منظمة هدفها اختراق النظم الإلكترونية المعقدة لتنفيذ عمليات السرقة الإلكترونية[1].

(1)http://www.pcintv.com/forums/showthread.php?t=14543

المبحث الثاني

ماهية سرية المعلومات الإلكترونية

نناقش في هذا المبحث بيان ماهية سرية المعلومات الإلكترونية وذلك ببيان ماهية المعلومات الإلكترونية وعناصرها وطبيعتها ، ومتى تكون المعلومات سرية ، وتحديد صاحب الحق في سرية المعلومات الإلكترونية، وتحديد المعلومات محل الحماية.

المطلب الأول

مفهوم المعلومات

قبل الخوض في موضوع البحث - الحماية الجنائية لسرية المعلومات الإلكترونية- يتعين أن نستجلي بداءة ماهية المعلومات الإلكترونية من حيث؛ مفهومها، وعناصرها، وطبيعتها القانونية، إذ إنه من الأهمية تحديد ماهية الشيء محل الحماية – المعلومات الإلكترونية - ليتسنى فهمها على نحو يمكننا من توفير الحماية اللازمة لها.

وفي ضوء ما تقدم سنتناول في هذا المطلب مفهوم المعلومات الإلكترونية، وبيان عناصرها، وطبيعتها القانونية باعتبارها محلا للاعتداء عليه.

الفرع الأول

تعريف المعلومات

قد يبدو للوهلة الأولى أن مفهوم المعلومات واضح وجلي، ولا يثير صعوبة، فمن منا لا يعرف ما هي المعلومة بوجه عام، إلا أنه عندما نتناول المعلومات الإلكترونية باعتبارها محلاً للحماية الجنائية فأنه ينبغي وضع مفهوم واضح ومحدد ، يمثل في الوقت ذاته تحديداً لنطاق الحماية الجنائية، وهو ما تتطلبه سياسة التجريم، لذا سنحاول في هذا الفرع بيان مفهوم المعلومات من الناحيتين اللغوية والاصطلاحية وذلك في ضوء الاجتهادات الفقهية والاتجاهات التشريعية المختلفة.

أولا - تعريف المعلومات لغة:

يقصد بالمعلومات لغة: الإخبار أو كل ما يؤدي إلى كشف الحقائق أو إيضاح الآمر [1].

ويقابلها في اللغة الإنجليزية كلمة Information[2] وتعني الحقائق عن موضوع معين أو شخص أو حدث معين.

ثانياً: تعريف المعلومات اصطلاحا:

تعددت التعريفات التي تناولت المعلومات نذكر منها ما يأتي :

- (الحقائق أو الإشارات أو الرسائل أو المفاهيم التي تعرض بطريقة صالحة للإبلاغ أو التوصيل أو التفسير بواسطة إنسان أو أدوات ومعدات آلية.)[3]

- (مجموعة من الرموز أو الحقائق أو المفاهيم أو التعليمات التي تصلح لأن تكون محلا للتبادل والاتصال أو للتفسير والتأويل أو للمعالجة سواء بواسطة الأفراد أو الأنظمة الإلكترونية، وهي تتميز بالمرونة بحيث يمكن تغييرها، وتجزئتها، أو نقلها بوسائل وأشكال مختلفة)[4]

- ويعرف البعض المعلومة بأنها (رسالة ما معبر عنها في شكل يجعلها قابلة للنقل أو الإبلاغ للغير)[5]

بعد تناولنا مفهوم المعلومات على النحو المتقدم، قد يثار تساؤل وهو، هل المعلومات هي البيانات ؟ بمعنى آخر، هل هما مترادفان؟ أم هناك اختلاف بينهما؟ وإذا كان هناك اختلاف بينهما فهل لهذا الاختلاف أثر على نطاق الحماية الجنائية للمعلومات الإلكترونية بحيث تشمل إحداهما دون الآخرى؟

وإجابة عن هذا التساؤل نبين أن هناك فريقاً يذهب إلى التمييز بين كل من المعلومات والبيانات، حيث يعرف البيانات بأنها مجموعة من الكلمات والرموز

---

(1) الأسيل – القاموس العربي الوسيط – دار الراتب الجامعية – الطبعة الاولى 1997 بيروت صـ677

(2) Information facts about a situation, person, event, etc- (Cambridge learner's Dictionary)

(3) د- محمد علي العريان – الجرائم المعلوماتية – مرجع سابق - صـ36

(4) د.نائلة عادل محمد فريد قورة – مرجع سابق صـ 93

(5) سامي علي حامد عياد – الجريمة المعلوماتية وإجرام الإنترنت – دار الفكر الجامعي – الإسكندرية 2007 – صـ24

أو الأرقام أو الحقائق أو الإحصاءات الخام تخلو من المعنى الظاهر والتي لم تخضع لعملية تفسير أو تجهيز .أما المعلومات فهي المعنى الذي يستخلص من هذه البيانات[1].

فالبيانات مجموعة من المعطيات والحقائق غير مرتبة (خام) ، أما المعلومات فهي نتيجة تحليل وتلخيص البيانات وتصنيفها وتجميعها بطريقة معينة، بواسطة النظام المعلوماتي بحيث تثمر عن معنى محدد يمكن الاستفادة منه، مما يزيد من قيمتها بالنسبة للمستفيد أو المستخدمين. وعلى هذا النحو يمكن القول بأن البيانات هي مدخلات النظام المعلوماتي ، والمعلومات هي مخرجاته.[2]

وقد تبنت التوصية الصادرة عن منظمة التعاون الاقتصادي والتنمية عام 1992 الخاصة بحماية أنظمة الحاسبات الآلية وشبكات المعلومات هذه التفرقة حيث عرفت البيانات بأنها (مجموعة من الحقائق أو المفاهيم أو التعليمات تتخذ شكلاً محدداً يجعلها قابلة للتبادل وللتفسير أو المعالجة بواسطة الأفراد أو بوسائل إلكترونية. أما المعلومات فهي المعنى المستخلص من هذه البيانات)[3]

بينما يذهب اتجاه آخر إلى عدم التمييز في مجال الحماية الجنائية بين المصطلحين ويعتبر كل منهما مرادفاً للثاني، ولا يرى مسوغاً أو فائدة ملموسة من التمييز بينهما على أساس أن المعلومات هي المعنى المستخلص من البيانات وبالتالي فإن الحماية الجنائية تشملهما معاً[4].

ومن جانبي، فإننا نؤيد الاتجاه الأخير، ولا نرى للتمييز بينهما أثراً على نطاق الحماية الجنائية للمعلومات، وأنها تشمل من الناحية الفعلية كلاً من المعلومات والبيانات، فكما أشرنا سالفا أن المعلومات هي المعنى الذي يمكن الاستفادة منه، وهي ثمرة أو نتيجة تحليل وتلخيص البيانات وتصنيفها وتجميعها، بواسطة

---

(1) أ. محمد عبدالله ابو بكر سلامة - موسوعة جرائم المعلوماتية (جرائم الكمبيوتر وانترنت) - منشاة المعارف - الإسكندرية 2006- صـ73

(2) د.يحي مصطفى حلمي - أساسيات نظم المعلومات - مكتبة عين شمس - القاهرة 1998- صـ72

(3) د.نائلة عادل محمد فريد قورة - مرجع سابق - صـ 94

(4) المرجع نفسه - صـ 94

النظام المعلوماتي، وبالتالي فإن كلاً منهما انصهر واندمج مع الآخر وشكلا سويا كياناً واحداً هو المعلومات الإلكترونية محل الحماية الجنائية. ونستدل على ذلك بما ذهبت إليه التشريعات المختلفة عند تعريفها للمعلومات:

- فعرفت المادة رقم (1) من المرسوم بقانون رقم (28) لسنة 2002 بشأن المعاملات الإلكترونية البحريني المعلومات بأنها (البيانات والنصوص والصور والأشكال والأصوات والرموز وبرامج الحاسب والبرمجيات وقواعد البيانات والكلام و ما شابه ذلك.) ،

- وعرفت المادة الأولى الفقرة (4) من نظام مكافحة الجرائم المعلوماتية السعودي البيانات بأنها (المعلومات، أو الأوامر، أو الرسائل، أو الأصوات، أو الصور التي تعد، أو التي سبق إعدادها، لاستخدامها في الحاسب الآلي، وكل ما يمكن تخزينه، ومعالجته، ونقله، وإنشاؤه بوساطة الحاسب الآلي، كالأرقام والحروف والرموز وغيرها) ،

- وعرفت المادة رقم (1) من القانون الاتحادي الإماراتي رقم 2 لسنة 2006 في شأن مكافحة جرائم تقنية المعلومات الإلكترونية بأنها: (كل ما يمكن تخزينه ومعالجته وتوليده ونقله بوسائل تقنية المعلومات وبوجه خاص الكتابة والصور والصوت والأرقام والحروف والرموز والإشارات وغيرها.)

- بينما عرف قانون حماية البيانات الانجليزي لسنة 1998 البيانات بأنها المعلومات التي بجري معالجتها بواسطة معدات التشغيل التلقائية استجابة لتوجيهات أعطيت لهذا الغرض [(1)].

- وعرف قانون المعاملات التجارية الإلكترونية الأمريكي لسنة 1999 المعلومات بأنها (تشمل البيانات والكلمات والصور والأصوات والرسائل

---

(1) **Data Protection Act 1998** (1Basic interpretative provisions (1)In this Act, unless the context otherwise requires—"data" means information which— (a) is being processed by means of equipment operating automatically in response to instructions given for that purpose,....)

وبرامج الكمبيوتر والبرامج الموضوعة على الأقراص المرنة وقواعد البيانات أو ما شابه ذلك)[1]

ومما تقدم نخلص إلى الأتي:

1- أن المعلومات هي المعنى الذي يمكن الاستفادة منه، وهي ثمرة أو نتيجة تحليل وتلخيص البيانات وتصنيفها وتجميعها، بواسطة النظام المعلوماتي.

2- أن غالبية التشريعات لا تميز بين المعلومات والبيانات في مجال الحماية الجنائية للمعلومات بل تعد كلاً منهما مرادفاً للآخر، حيث أن التشريعات لتي تبنت مصطلح المعلومات، عرفتها بأنها البيانات، والتشريعات التي تبنت مصطلح البيانات عرفتها، بأنها المعلومات.

3- أن المعلومات الإلكترونية: لا تقتصر على شكل معين فقد تكون صوراً أو كلمات أو أصواتاً أو أرقاماً أو حروفاً أو رموزاً، أو رسائل أو برامج حاسب آلي وكذلك البرمجيات وقواعد البيانات وكل ما يمكن تخزينه ومعالجته وتوليده ونقله بوسائل تقنية المعلومات.

4- أن معظم التشريعات عددت صور وأشكال المعلومات المشار إليها في البند السابق على سبيل المثال لا الحصر ، بحيث يتسع النص لأي أشكال أو صور قد تظهر مستقبلا للمعلومات،وحسنا فَعَلت، إذ أن هذا التوجه يتفق مع ما يمتاز به عالم تكنولوجيا المعلومات من سرعة في التطور، وهو ما ينبغي على كل مشرع أخذه بعين الاعتبار عند سن التشريعات الخاصة بالجرائم المعلوماتية.

---

(1) د.خالد ممدوح إبراهيم - الجرام المعلوماتية - دار الفكر الجامعي - الإسكندرية 2009 ، ص50

الفرع الثاني

عناصر المعلومات

بعد تعريف المعلومات على النحو المتقدم، نتناول في هذا الفرع عناصر المعلومات الإلكترونية، فلكي تتمتع المعلومة بالحماية الجنائية ينبغي أن تتوافر فيها العناصر الآتية:

1 – التحديد:

يجب أن تكون المعلومة محددة، وهذا ما يتفق مع تعريف المعلومات من حيث كونها مجموعة من الرسائل والحقائق والمفاهيم وعند انتقالها بين الأشخاص فإنه يتم تبليغها لتوصيل رسالة أو معنى محدد. وتكون المعلومة محددة عندما يمكن حصرها في دائرة أو نطاق خاص بها. وهذا التحديد ضرويٌّ لاعتبار المعلومات حق، فمحل الحق يجب أن يكون محدداً، ناهيك عن أن الحماية الجنائية يجب أن تنصب على شيء محدد بحيث يشكل الاعتداء عليه جريمة جنائية.

2 – الابتكار:

الابتكار لغةً يعني الاختراع. وبالنسبة للمعلومات هو أن تتسم المعلومة بالأصالة والحداثة بمعنى أنها لم تكن موجودة من قبل، فالمعلومة الشائعة والمتاحة للجميع والتي لا يمكن نسبتها لشخص محدد لا يمكن اعتبارها معلومة بالمعنى الفني الدقيق[1]. كما أنه في تقديري لولا انطلاء صفة الابتكار على المعلومة ما كانت لتصلح أن تكون محلا للحماية الجنائية ، إذ أن الابتكار هو ما جعل من تلك المعلومة حقاً أو ملكاً لصاحبها وبالتالي فإن أي اعتداء على هذا الحق يشكل جريمة،على خلاف المعلومة العامة المتاحة للكافة.

3 – السرية:

يقصد بالسرية أن المعلومة تدور في نطاق محدود من الأشخاص وبعكس ذلك فإذا كانت المعلومة عامة وشائعة فإنها بطبيعتها لا يمكن أن تكون محلا

---

(1) د. محمد علي العريان – مرجع سابق ص 40

للسرقة أو الاعتداء. أو انتهاكا للخصوصية.

وقد تستمد المعلومة سريتها إما بإرادة صاحبها باكتشاف في مجال حديث أو بحسب طبيعتها كاكتشاف شيء لم يكن موجوداً ، أو للسببين معا كما هو الحال بالنسبة للرقم السري لبطاقة الائتمان.[1] وسنتناول موضوع السرية على نحو أكثر تفصيلا في المطلب الثاني.

4- الاستئثار:

يقصد بالاستئثار فأنه يعني أن شخصاً معيناً هو من يحوز تلك المعلومة بحيث لا يمكن الحصول على تلك المعلومة دون تصريح من صاحبها. كما هو الحال بالنسبة لمؤلف المعلومة إذ تعد المعلومة ملكا له [2]، وبالتالي فإن عنصر الاستئثار يعد عنصراً لازماً لاعتبار أي اعتداء على تلك المعلومة هو من قبيل الاعتداء على ملك الغير المعاقب عليه قانونا.

إذا فالاستئثار هو اختصاص الشخص بشيء معين و استقلاله به علي سبيل التفرد، فالمالك في حق الملكية يستأثر بمحل الملكية.

---

(1) د.نائلة عادل محمد فريد قورة مرجع سابق صـ 109

(2) المرجع نفسه صـ 110

المطلب الثاني

الطبيعة القانونية للمعلومات

اختلف الفقهاء بشأن الطبيعة القانونية للمعلومات ومن حيث مدى كون المعلومات تمثل قيمة مالية في ذاتها من عدمه، وسنتناول بالدراسة في هذا الفرع بحث مدى اعتبار المعلومات مالاً من وجهتي الشريعة الإسلامية والقانون وذلك على النحو الآتي:

الفرع الأول

القيمة المالية للمعلومات في الشريعة الإسلامية

يعرف المال لغة بأنه: ما ملكته من جميع الأشياء، وجمعه أموال[1]

واصطلاحاً: انقسم الفقه الإسلامي في تعريف المال إلى اتجاهين الأول للحنفية، والاتجاه الثاني لجمهور الفقهاء (المالكية والشافعية والحنابلة) وبيان ذلك على النحو الآتي:

1- تعريف المال عند الحنفية:

عرف الحنفية المال بتعريفات عديدة أهمها[2] :

- ما يدخر للانتفاع به وقت الحاجة.
- ما خلق لمصالح الآدمي، وأمكن إحرازه والتصرف فيه على وجه الاختيار.
- ما يميل إليه الطبع ويجري فيه البذل والمنع.

وفي ضوء التعريفات المتقدمة فإنه يشترط وفقا لاتجاه الحنفية حتى يعتبر الشيء مالاً أن تتوافر فيه العناصر التالية مجتمعة[3]:

---

(1) أبو الفضل جمال الدين محمد بن مكرم بن منظو، لسان العرب، 11/ 635 – 636 – مطبعة دار صادر بيروت – الطبعة (1) سنة 1410 هـ

(2) د.نذير بن محمد الطيب أوهاب - حماية المال العام في الفقه الإسلامي – اكاديمية نايف العربية للعلوم الأمنية - الرياض – الطبعة الأولى 2001- صـ 10-13

(3) عبدالـله بن حمد بن ناصر العطميل - أحكام تنف الأموال في الفقه الإسلامي -- المملكة العربية السعودية – 1408 هـ / 1988م – صـ 22

أ- أن يكون منتفعا به في حال السعة والاختيار دون حال الضرورة.

ب- أن يكون شيئا موجوداً في زمانين فأكثر، وهو ما قصده فقهاء الحنفية بعبارة (ما يدخر للانتفاع به وقت الحاجة) ويقصدون من ذلك آخراج المنفعة من وصف المال.

ج- أن يكون له قيمة مادية بين الناس، فكل ما لا يمكن الانتفاع به أصلا، كلحم الميت والطعام المسموم أو الفاسد، أو ينتفع به انتفاعا لا يعتد به عادة عند الناس، كقطرة ماء، لا يعد مالاً.

ح- أن يكون ممكن الحيازة والإحراز؛ فالماء، والطير في الهواء والسمك في الماء قبل الإحراز، فالقيمة عندهم لا تسبق الإحراز، ولا يعد مالاً ما لا يمكن حيازته كالأمور المعنوية مثل العلم والمعرفة.

ولما كانت المعلومات ذات طبيعة معنوية لا يمكن حيازتها وادخارها، فإنها بذلك تكون قد فقدت أحد عناصر المال وفقا للاتجاه الحنفية وبالتالي لا تعد مالاً في حد ذاتها، إلا أنها قد تعد كذلك في حالة ما إذا تم إفراغها في وسيط مادي كالكتب، أو وسائط التخزين الإلكترونية، حيث إنها في هذه الحالة تكون كالسمك بعد اصطياده من الماء، تكون قد أحرزت وبالإمكان حيازتها وادخارها، فضلا عن توافر باقي عناصر المال بها.

2- تعريف المال عند الجمهور الفقهاء (المالكية والشافعية والحنابلة):

أ- تعريف المال عند المالكية : (هو ما يقع عليه الملك ويستبد به المالك عن غيره إذا أخذه من وجهه)[1]

ب- تعريف المال عند الشافعية: عرف الإمام الشافعي المال بقوله (لا يقع المال إلا على ما له قيمة يباع بها، وتلزم متلفه، وإن قلت، وما لا يطرحه الناس مثل الفلس، وما شابه ذلك)[2]، ويعرف أبو عبدالله محمد بن بهارد الزركشي

---

(1) عبدالله بن حمد بن ناصر الغطميل- مرجع سابق صـ25

(2) جلال الدين عبدالرحمن بن أبي بكر السيوطي، الأشباه والنظائر، الطبعة الأخيرة ، مطبعة مصطفى بأبي الحلبي 1378هـ- صـ327

المال بأنه (ما كان منتفعا به) وبين أن المقصود بالانتفاع ما ينتفع به وهو إما أعيان أو منافع. وقيدوا الانتفاع بالإباحة، بحيث يخرج ما منفعته محرمة.[1]

ج- تعريف المال عند الحنابلة[2]:

- ما فيه منفعة مباحة لغير حاجة أو ضرورة

- ما يباح نفعه مطلقاً في كل الأحوال أو يباح اقتناؤه بلا حاجة.

وعناصر المال عند الحنابلة تتلخص في الآتي:

أ- أن يكون فيه منفعة مقصودة مباحة شرعا في غير حاجة أو ضرورة،

ب- أن يكون له قيمة مادية بين الناس.

ونستخلص من تعريفات الجمهور: أن المال هو ما فيه منفعة مقصودة مباحة شرعا في غير ضرورة أو حاجة،ويجري فيه البذل والمنع.

فإذا انطبق هذا التعريف على شيء ما صح أن يطلق عليه اسم المال دون اشتراط إمكان الادخار لوقت الحاجة كما ذهب الحنفية، والذين أخرجوا المنافع عن مفهوم المال.

وفي رأيي، وحيث إننا أضحينا في عصر أصبحت فيه المعلومات تتمتع فيه بقيمة اقتصادية كبيرة، تدر نفعا على مقتنيها، ويبذل من أجلها المال في سبيل الحصول عليها، بل إن المعلومات أضحت تشكل أحد أهم أصول فروع الاقتصاد الجديد والذي يعرف (باقتصاد المعرفة) [3]، عليه فإن المعلومات تكون قد توافر فيها عناصر المال التي اتفق عليها جمهور الفقهاء على النحو المتقدم بيانه.

---

(1) د.نذير بن محمد الطيب أوهاب ، مرجع سابق صـ15.

(2) عبدالله بن حمد بن ناصر الغطميل- مرجع سابق صـ30

(3) أصبحت الأصول المهمة في الاقتصاد الجديد هي المعرفة الفنية، والإبداع، والذكاء، والمعلومات. وتقدر الأمم المتحدة أن اقتصادات المعرفه تستأثر الآن 7 ٪ من الناتج المحلي الاجمالي العالمي وتنمو بمعدل 10 ٪ سنويا. كما ان 50 ٪ من نمو الإنتاجية في الاتحاد الأوروبي هو نتيجة مباشرة لاستخدام وإنتاج تكنولوجيا المعلومات والاتصالات – راجع: http://ar.wikipedia.org/

الفرع الثاني

القيمة المالية للمعلومات في القانون

انقسم فقهاء القانون أيضا بالنسبة لتحديد الطبيعة القانونية للمعلومات وما إذا كانت تتمتع بقيمة مالية إلى فريقين:

- الفريق الأول : يذهب أنصاره إلى أن المعلومات ذات طبيعة خاصة ولا يمكن إطلاق وصف القيمة عليها واعتبارها من القيم المالية التي يمكن الاعتداء عليها.إذ أن الأشياء المادية هي من توصف بالقيمة فقط، انطلاقا من أن الأشياء التي توصف بالقيم هي الأشياء التي تقبل الاستحواذ عليها[1] وتكون قابلة للتملك. وعليه فإنه لما كانت المعلومات ذات طبيعة معنوية لا يمكن الاستئثار بها فإنها لا تدخل ضمن طائفة القيم المشمولة بالحماية ما لم تكن تنتمي إلى مجموعة المواد الفنية والأدبية والتي تحميها حقوق الملكية الأدبية والفنية والفكرية. غير أن هذا الفريق في الوقت نفسه لا ينكر على المعلومات قيمتها الاقتصادية، مما حدا بالبعض إلى اعتبارها من طائفة المنافع والخدمات.

وعلى الرغم مما تقدم فقد ظهرت محاولات لأنصار هذا الفريق لتوفير الحماية القانونية للمعلومات، لذا فقد لجؤوا في بعض الأحيان إلى استعمال دعوى المنافسة غير المشروعة، والتطبيق الموسع لنظرية التصرفات الطفيلية ، نظرية الإثراء بلا سبب، وأخيرا استندوا إلى نظرية المسئولية التقصيرية [2]

- الفريق الثاني: يرى أنصار هذا الفريق أن المعلومات ذات قيمة مالية تتشابه في ذلك مع غيرها من القيم الآخرى، وأخذ بهذا الاتجاه الفقيهان الفرنسيان Catala و Vivant [3].

فالفقيه Catala يرى أن المعلومات بذاتها قيمة مالية ويمكن أن تصبح قيمة

---

(1) محمد علي العريان – مرجع سابق صـ49

(2) د.نائلة عادل محمد فريد قورة – مرجع سابق صـ111

(3) د. محمد علي العريان – مرجع سابق صـ50

قابلة للتملك في ذاتها بصرف النظر عن الوسيط المادي الذي يحتويها ، وقد شبهها بالسلعة من حيث أن كليهما نتاج لعمل بشري وتنتمي إلى من يحوز عناصرها بطريقة مشروعة ، ومن ثم يضعها في أي هيئة تكون معها صالحة للإطلاع عليها وتناقلها وتبليغها. وقد استند إلى حجتين رئيسيتين:

الأولى: القيمة الاقتصادية للمعلومات والتي يمكن أن تقوم بالمال وبسعر محدد.

الثانية: علاقة التبعية التي تربط المعلومة بمؤلفها وهي العلاقة القانونية التي تربط المالك بالشيء المملوك.[1]

وبدوري أؤيد ما ذهب إليه الفقيه Catala، فالمعلومة خاصة في الوقت الحالي تتمتع ذات قيمة وتُقوَم بالمال مثلها مثل أي سلعة آخرى، ويتم التعامل عليها حتى أضحى هناك ما يسمى بسوق المعلومات، أو سوق الأفكار.

وقد أيد الفقيه Vivant ما ذهب إليه Catala من حيث أن للمعلومات قيمة اقتصادية في ذاتها وهي قابلة للتملك ، ويستدل على تلك القيمة بأن الملكية الفكرية وبراءات الاختراع والرسومات وغيرها من الأشياء المملوكة ملكية معنوية والتي تقوم على أساس وأحد وهو أن للمعلومة قيمة من الناحية القانونية.

---

(1) د.نائلة عادل محمد فريد قورة - مرجع سابق صـ115

المطلب الثالث

مفهوم السر

تعد السرية إحدى الأهداف الأساسية لأمن المعلومات بالإضافة إلى السلامة والتكامل، والتوفر. فالسرية يقصد بها أن المعلومات السرية يجب أن تبقى خاصة بمالكها أو من له سلطة قانونية عليها سواء كان شخصاً طبيعياً أو معنوياً، وأن تحفظ تلك المعلومات من الاطلاع والكشف الغير المصرح به أو المفاجئ من قبل أشخاص غير مصرح لهم بالاطلاع عليها أو الكشف عنها. مثال على ذلك التعامل ببطاقات الائتمان والمعاملات التجارية والمعاملات البنكية على شبكة الإنترنت يتطلب إدخال الرقم السري لبطاقة الائتمان على الموقع الإلكتروني وهو ما يتطلب ضمان السرية خلال انتقال البيانات من المشتري إلى التاجر ومن التاجر لإنجاز وتجهيز المعاملات على الشبكة وذلك عن طريق تشفير رقم البطاقة أثناء الإرسال، والعمل قدر المستطاع على عدم ظهور تسلسل رقم البطاقة في قواعد البيانات، وسجل الملفات، النسخ الاحتياطي، والإيصالات المطبوعة، وذلك بمنع الوصول إلى الأجزاء التي يتم تخزين الرقم والبيانات بها. أما السلامة والتكامل فتعني الحفاظ على البيانات من التغيير والتعديل من قبل الأشخاص الغير مصرح لهم بذلك. كأن يقوم شخص غير مصرح له بالمساس بسلامة أو حذف البيانات أو المعلومات المخزنة.أما التوفر فينعي ضمان الوصول إلى المعلومات والبيانات المخزنة إلكترونياً وأن تكون تلك المعلومات أو البيانات متوفرة بسهولة. فحتى يحقق أي نظام معلوماتي أهدافه ، يجب أن تكون المعلومات متوفرة عند الحاجة إليها. وهو ما يتطلب أن تكون الأنظمة المعلوماتية المستخدمة لتخزين ومعالجة المعلومات، وقنوات الاتصال المعتمدة للوصول إليها والضوابط الأمنية المستخدمة لحمايته،تعمل بكفاءة وبشكل صحيح وبصورة مستمرة وفي جميع الأوقات، ومنع انقطاع الخدمة لأي سبب كانقطاع التيار الكهربائي، أو تعطل الأجهزة، كما يتطلب ضمان توافر

التصدي لهجمات أو محاولات الحرمان من الخدمة [1]

وسنتناول في هذا المطلب مفهوم السر ومن هو صاحب الحق في سرية المعلومات الإلكترونية، وموقف الشريعة الإسلامية من حماية سرية المعلومات باعتبارها أحد المصادر الرئيسة للتشريع بموجب الدستور.

---

(1) سمان بن علي بن وهف القحطاني - أمن المعلومات في ضوء التطور التقني والمعلوماتي الحديث في الشبكات اللاسلكية النقالة – بحث مقدم في المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية 26 /2003/4- 2003/4/28 دبي – الأمارات العربية المتحدة – صـ13 ، وانظر أيضاً الموقع الالكتروني http://ar.wikipedia.org- مقال بعنوان أمن المعلومات.

الفرع الأول

تعريف السـر

أولا: التعريف اللغوي للسـر :

يعرف السـر لغة : (السـر) ما يكتمه الإنسان في نفسه ، باطن الوادي[1].

والجهر ضد السـر ، فالإسـرار: عكس الإعلان، قال تعالى: { الَّذِينَ يُنْفِقُونَ أَمْـوَالَهُمْ بِاللَّيْـلِ وَالنَّهَارِ سِـرا وَعَلانِيَـةً فَلَهُـمْ أَجْـرُهُمْ عِنْـدَ رَبِّهِـمْ } (البقـرة/274) ، وقـال تعـالى: { وَأَسِـروا قَوْلَكُمْ أَوِ اجْهَرُوا بِهِ} [الملك/13]،

والسـر هو الحديث المكنون في النفس. وقوله تعـالى: { وَأَسـروا النَّدَامَـةَ} [يـونس/54]، أي: كتموها، ويقال أسـررت إلى فلان حديثا: أفضيت إليـه في خفيـة، وإن الأسـرار إلى الغـير يقتضي إظهار وبيان ذلك لمن يفضي إليه بالسر، وإن كان يتطلب إخفاءه عن غيره[2]. وقوله تعالى { يَوْمَ تُبْلَى السـرائِرُ} (الطارق/9) والسـرآئر جمـع سـريرة بمعنـى السـر وهـى التي تكتم وتخفى ، وهو ما أسـر في القلوب من العقائد والنيات وغيرها وما أخفي من الأعمال[3]

ثانيا: التعريف الاصطلاحي للسـر:

تفادت معظم التشـريعات وضع تعريفٍ للسـر ، ذلك أن تعريف أي مصطلح ينبغي أن يكون مانعاً جامعاً، وهو ما يتعذر على أي مشـرع بالنسبة لتعريف السـر ، فتحديـد السـر يختلف باختلاف الظروف، فما يعتبر سـرا في ظرف معين قد لا يعتـبر كـذلك في ظـرف آخـر، كما أن ما يعتبر سـرا بالنسبة لشخص ما قـد لا يعتـبر كـذلك بالنسـبة لشـخص آخـر، لـذلك نلاحظ انه عادةً ما يترك المشـرع مهمة تعريف السـر للفقهاء.

---

(1) الأسيل القاموس العربي الوسيط - دار الراتب الجامعية – بيروت - الطبعة الأولى1997 - صـ 371

(2) مفردات ألفاظ القرآن للحسين بن محمد المعروف بالراغب الأصفهاني أبي القاسم /http://islamport.com

(3) تفسير حقي- http://islamport.com

وفيما يلي نستعرض بعض تعريفات الفقه للسـر:

يعرف البعض السـر بأنه (أمر ما يتعلق بشخص المرء ويمس الدائرة الشعورية الحساسة من نفسه بحيث يكون في البوح به حرج كبير)[1]

ويعرفه البعض الأخر بأنه واقعة أو صفة ينحصر نطـاق العلـم بهـا في عـدد محـدد مـن الأشخاص، إذا كانت ثمة مصلحة يعترف بها القانون لشخص أو لأكـثر في أن يظـل العلـم بهـا محصورا في ذلك النطاق.[2]

كما يعرفه البعض أيضاً بأنه؛ أمر يتصل بشيء أو شخص من خاصيته أن يظل مجهـولاً أو غير معروفٍ لكل شخص غير مكلف قانوناً بحفظه أو اسـتخدامه ، بحيـث يكـون العلـم بـه مقصوراً على عدد محدد من الأشخاص هم الذين يكلفون بحفظه أو استخدامه.[3]

تم تعريف السـرية أيضا بواسـطة المنظمـة الدوليـة للتوحيـد القيـاسي (أيـزو) في أيـزو 17799 - عـلى أنهـا "ضـمان أن تكـون المعلومـات متاحـة فقـط لأولئـك الـذين يـؤذن لهـم بالإطلاع"[4]

---

(1) د. رمسيس بهنام ، قانون العقوبات - جرائم القسم الخاص ، منشأة المعارف ، الإسكندرية 1999 ، صـ1088

(2) د. محمود نجيب حسني ، شـرح قانون العقوبات - القسم الخاص ، دار النهضة العربية ،1986 صـ 753

(3) د.إبراهيم حامد طنطاوي، الحماية الجنائية لسـرية معلومـات البنـوك عـن عملائها في ضـوء القـانون رقـم 88 لسنة 2003 دراسة مقارنة، دار النهضة العربية 2005 ، صـ18

(4)http://ar.wikipedia.org/wiki/%D8%A7%D9%84%D8%B3%D8%B1%D9%8A%D8%A9

الفرع الثاني

صاحب الحق في سرية المعلومات الإلكترونية

كما سبق وبينا في معرض حديثنا عن القيمة القانونية للمعلومات، أن المعلومات بذاتها قيمة مالية ويمكن أن تصبح قيمة قابلة للتملك في ذاتها بصرف النظر عن الوسيط المادي الذي يحتويها.

وفي ضوء ذلك فإن صاحب الحق في سرية المعلومات الإلكترونية هو مالكها أو من له سلطة قانونية عليها تخوله الاستئثار بالمعلومات واستعمالها واستغلالها والتصرف فيها. سواء أكان شخصاً طبيعياً كمالك الفكرة أو المؤلف أو صاحب براءة الاختراع، أو شخصاً اعتبارياً كالشركات أو المؤسسات بالنسبة للأسرار التجارية أو البنكية والمالية، أو الدول بالنسبة لأسرار الدولة العسكرية أو السياسية أو الاقتصادية.

ويلاحظ أنه بالنسبة للأشخاص الاعتباريين، قد يطلع على المعلومات السرية الخاصة بها أو تلك المتعلقة بعملائها أكثر من شخص بحكم عمله،مثال الأسرار البنكية التي يطلع عليها موظفوا البنك أو أسرار التجارة أو الصناعة، إلا أن ذلك لا ينال من سرية تلك المعلومات طالماً أن كلاً منهم يتعامل معها في إطار من السرية والكتمان، وطالما ليست معلنة أو متاحة للكافة.

كما أنه يجوز لمالك المعلومة أو لمن له سلطة قانونية عليها الترخيص باستعمالها للآخرين ولا يؤدي ذلك إلى زوال صفة السرية، وذلك لالتزام المرخص له بالكتمان، مثال ذلك القنوات المشفرة، إذ إن المعلومات كما سبق وعرفناها قد تكون صوتاً أو صورة أو فيديو، وأن قيام مالك القنوات المشفرة باتخاذ التدابير اللازمة (التشفير) للمحافظ على سريتها بحيث لا يكون من المتاح للكافة الوصول إليها والاطلاع عليها دون الحصول على تصريح منه، وذلك بدفع قيمة الاشتراك المحدد لها، ويلاحظ أنه دائما ما يتم في الاشتراك تحديد شروط ونطاق هذا الاستخدام ومدته.

الفرع الثالث

المعلومات الإلكترونية السرية محل الحماية

المعلومات المستهدفة بالحماية الجنائية موضوع هذا البحث هي المعلومات الإلكترونية المعالجة إلكترونياً، ويقصد بها المعلومات المعالجة آليا بواسطة نظام معلوماتي أو أحد أجزاءه كالحاسب الآلي بهدف تصنيفها وإعادة إنتاجها وبثها أو تخزينها وتسجيلها سواء بواسطة أحد الأجزاء الداخلية للنظام المعلوماتي كذاكرة الحاسب مثلا، أو على وسائط تخزين خارجية كالأقراص المرنة (CD).

وتنقسم المعلومات الإلكترونية من حيث إمكانية الوصول إليها؛ إلى معلومات متاحة، ومعلومات سرية أو غير متاحة. وتلجأ عادة المواقع الإلكترونية إلى وضع سياسات واضحة بشأن تحديد المعلومات التي سيتم نشرها وإتاحتها للجميع، وتلك التي ستظل سرية من بين ما تحتفظ به من معلومات .

ويقصد بالمعلومات المتاحة تلك المعلومات والبيانات المنشورة على المواقع الإلكترونية المفتوحة للجمهور بحيث يمكنهم الدخول إليها والاطلاع على ما تحتويه من بيانات ومعلومات منشورة عليها كمعلومات البورصة مثل حركة الأسهم وعمليات البيع والشراء، وكذلك المقالات والأبحاث والكتب المنشورة بموافقة مالكيها على المواقع الإلكترونية.

وقد يكون من بين المعلومات المتاح للجمهور الاطلاع عليها تلك البيانات والمعلومات المنشورة من قبل الوزارات والمؤسسات الحكومية في حدود القانون، حيث تعمد بعض الدول إلى نشر بعض المعلومات والبيانات الحكومية في ضوء إقرار حق المواطن في الحصول على المعلومات،ومن الأمثلة على ذلك مشروع منصة البيانات المفتوحة الذي اعتمدته مملكة البحرين في إطار توجه المملكة إتاحة البيانات العامة للجمهور ووضع إستراتيجية للبيانات المفتوحة بهدف تعزيز الشفافية وتشجيع المشاركة الإلكترونية وتشجيع البحث العلمي، وتشجيع الاستثمار. ويتيح هذا المشروع مجموعات من البيانات المنشورة من قبل

مختلف الوزارات والجهات الحكومية بصيغ تسهل معالجتها وإعادة استخدامها[1]. وهذه الطائفة من المعلومات بطبيعة الحال تتمتع بالحماية الجنائية لضمان سلامتها وتوافرها، دون الحماية الجنائية لسريتها.

وبعبارة مختصرة فإن المعلومات الإلكترونية المتاحة هي المعلومات المنشورة على أحد المواقع الإلكترونية المفتوحة للعامة بتصريح من مالكيها أو من له سلطة قانونية عليها تخوله ذلك.

أما المعلومات الإلكترونية السرية أو غير المتاحة، فهي التي يقتصر العلم بها على شخص مالكها أو من يملك سلطة قانونية عليها، أو ينحصر العلم بها في نطاق عدد محدد من الأشخاص بحكم صلتهم القانونية بمالكها، ولا يكون متاحاً للكافة الوصول إليها والاطلاع عليها وحفظها واستخدامها أو استغلالها دون شرط أو قيد، نتيجة للتدابير التي اتخذها مالك المعلومة للمحافظة على سريتها، وبحيث يكون هو وحده من يملك الوصول إليها أو يمنح التصريح بالوصول إليها والاطلاع عليها واستخدامها، وتكون المعلومات الإلكترونية سرية أيضاً إما بطبيعتها أو طبقاً للقانون مثل المعلومات المتعلقة بالأسرار الخاصة بالدفاع الوطني أو أمن الدولة أو سياستها الخارجية، أو المعلومات المتعلقة بالأسرار التجارية أو المصرفية والبنكية أو حقوق الملكية الفكرية، أو المعلومات الشخصية المتعلقة بسجلات الأشخاص التعليمية أو الطبية أو حساباتهم أو تحويلاتهم المصرفية أو أسرار مهنتهم. أو المعلومات المتعلقة بالمراسلات ذات الطبيعة الشخصية والسرية والتي تتم عبر البريد الإلكتروني ووسائل تقنية المعلومات. وعادة ما تكون أنظمة المعلومات التي تحتوي مثل هذه البيانات والمعلومات محاطة بنوع من الحماية لمنع الوصول والاطلاع عليها أو تعديلها أو إتلافها من قبل أشخاص غير مصرح لهم بذلك .

---

(1) الموقع الالكتروني لمنصة البيانات المفتوحة - مملكة البحرين http://www.data.gov.bh

المبحث الثالث

صور الجرائم المعلوماتية الماسة بسرية المعلومات الإلكترونية

أدى الاعتماد المتزايد على نظم المعلومات الإلكترونية في جمع المعلومات الخاصة بالأفراد مثل الوضع المادي أو الصحي أو الانتماء السياسي أو الديني، وكذلك المعلومات الخاصة بالشركات والمؤسسات والدول، وتخزينها ومعالجتها وتحليلها والربط بينها واسترجاعها ، إلى تعرض تلك المعلومات والبيانات لعدة مخاطر وأفعال إجرامية تمس سلامتها وسريتها حيث يستهدف مرتكبي هذه الأفعال الوصول إليها بغير تصريح أو استئذان، وكلما زادت قيمة تلك المعلومات زادت محاولات الوصول إليها، فضلا عن أن شيوع أسلوب النقل الرقمي للمعلومات والبيانات عن طريق شبكات الاتصال جعلها عرضة أكثر من ذي قبل للتجسس الإلكتروني عن طريق الاعتراض والالتقاط غير القانوني لتلك المعلومات.

وبالإضافة إلى الوسائل الفنية والتقنية، تعد الحماية القانونية أحد أهم خطوط الدفاع عن أمن المعلومات الإلكترونية ،من المخاطر التي تتعرض لها، وفي ضوء ذلك سوف نتناول في هذا المبحث صور الجرائم الماسة بسرية المعلومات الإلكترونية وهي الوصول غير القانوني أو البقاء غير القانوني داخل النظام المعلوماتي وجريمة الاعتراض غير القانوني للبيانات، من حيث وسائل ارتكاب كل جريمة وأركانها في ضوء التشريعات القانونية المختلفة

المطلب الأول

جريمة الدخول (الولوج)غير القانوني للنظام المعلوماتي

سبق وأن ذكرنا أن الحاسبات الآلية والشبكات المعلوماتية قد أصبحت مستودعا لكثير من أسرار البشر مما جعل منها هدفا ومطمعاً لكثير من مجرمي المعلومات، أو المتطفلين الفضوليين الذين يجدون متعتهم في اختراق النظم المعلوماتية والاطلاع على ما تحتويه من أسرار والعبث بها.

وعلى الرغم مما للتقدم والتطور التقني اللامتناهي في مجال التكنولوجيا ووسائل الاتصالات من انعكاسات ايجابية على مختلف جوانب حياة المجتمعات، إلا أنه في الوقت ذاته ونتيجة لإساءة استغلاله من قبل البعض أصبح يشكل تهديدا خطيرا لخصوصية الأفراد، وأسرار الدول والمؤسسات والشركات. وقد سهل هذا التطور مهمة مجرمي المعلومات وساعد على زيادة قدرتهم في الوصول إلى المعلومات المخزنة إلكترونيا والاطلاع عليها والعبث بها وإفشائها. وزاد من قدرتهم على التخفي ومحو آثار جرائهم على نحو يصعب معه ضبطهم وبالتالي تمكنهم من الإفلات من العقاب. وأمام تلك المخاطر والتهديدات عمدت مختلف الأنظمة القانونية إلى منح أجهزة الحاسب الآلي والشبكات المعلوماتية الحرمة والحماية التي تتناسب مع أهميتهما في العصر الحالي كمستودع للأسرار، وذلك بتجريم الدخول غير القانوني أو البقاء غير القانوني داخل النظم المعلوماتية.

وفي تقديري، يعد فعل الدخول غير القانوني من أبرز التهديدات التي تواجه المعلومات المعالجة إلكترونيا ،فهو بمثابة الشرارة الأولى أو البوابة لارتكاب غيره من الجرائم المعلوماتية مثل جرائم نقل وسرقة البيانات أو إتلافها أو تزويرها، ذلك أن تلك الجرائم في كثير من الأحيان تتطلب الدخول إلى النظام المعلوماتي والذي غالباً ما يكون غير مشروع ، إذا من المتصور أن تقع تلك الجرائم من قبل أفراد لهم صلاحية الدخول إلى النظام المعلوماتي بحكم

وظيفتهم، فيستغلوا تلك الصلاحية لارتكاب جرائمهم داخل النظام المعلوماتي. ومما يزيد من خطورة فعل الدخول غير القانوني، أنه قد يتسبب في خسائر مادية كبيرة للمجني عليه، وخاصة إذا كان الموقع الإلكتروني أو النظام المعلوماتي يعود إلى أحد البنوك أو المؤسسات المالية أو الشركات الذي يشكل عنصر الزمن والسرعة في الإنجاز أحد عوامل ربحها وخسارتها، فعادة ما يتعمد الجاني خلال محاولاته للدخول إحداث ثغرات في النظام المعلوماتي أو تعطيل أجزاء منه أو تعطيل الموقع، وهو ما قد يؤدي إلى إعاقة خدمات النظام المعلوماتي أو الموقع وبالتالي فوات فرص الربح على الشركة أو البنك مالك النظام أو الموقع المعتدى عليهما.

ولقد تضمنت المذكرة التفسيرية لاتفاقية بودابست المتعلقة بالجرائم الإلكترونية في تعليقها على المادة الثانية والخاصة بـ (الولوج غير القانوني) أنه كمبدأ عام يعتبر الدخول غير المصرح به بمعنى (القرصنة) أو (السطو) أو (الدخول غير المشروع في النظام المعلوماتي) مجرم أو غير قانوني، وذلك نظرا لما ينجم عن هذه الأفعال من عقبات تحول بين المستخدمين الشرعيين والانتفاع من النظم المعلوماتية والبيانات ولما قد يترتب عليها من إتلاف أو تدمير يتطلب مبالغ طائلة لإعادة بنائه. وأن هذا الدخول يؤدي إلى الوصول إلى بيانات سرية، كما أنها تشجع المخترقين (الهاكرز) على ارتكاب أنواع أكثر خطورة من الجرائم ذات الصلة بالحاسب الآلي.[1]

ومن أمثلة ذلك قضية (الجحيم العالمي Global Hell) وملخص هذه القضية قيام مجموعة من الأشخاص باختراق مواقع البيت الأبيض والشركة الفدرالية الأمريكية والجيش الأمريكي ووزارة الداخلية الأمريكية، وتم إدانة اثنين من أفراد هذه المجموعة ، وظهر من التحقيقات أن الدافع وراء ارتكاب هذه المجموعة لجريمتهم هو مجرد الاختراق أكثر من التدمير أو التقاط المعلومات، وقد تطلب الوصول إلى هذه المجموعة مئات الساعات بين

---

(1) نقلا عن د. هلالي عبدالله احمد – مرجع سابق صـ 69-70

ملاحقتها وتتبع آثار أنشطتها، وكلف التحقيق في هذه القضية مبالغ طائلة نظرا لما تطلبه من وسائل معقدة في المتابعة[1].

لكل ما تقدم فقد حرصت كثير من الدول على تجريم أفعال الدخول غير القانوني للنظام المعلوماتي بموجب تشريعاتها الجزائية، فضلا عن الاتفاقيات الإقليمية أو الدولية مثل اتفاقية بودابست المتعلقة بالجريمة الإلكترونية. وبغية إيلاء الموضوع حقه من الإيضاح سنستعرض في هذا المطلب جريمة الدخول غير القانون من حيث بيان مفهوم الدخول غير المصرح به ووسائله، وأركان هذه الجريمة وذلك في ضوء التشريعات القانونية المختلفة.

---

(1) د.عبدالفتاح مراد - شرح جرائم الكمبيوتر والانتر نت - شركة البهاء لبرمجيات والكمبيوتر والنشر اللالكتروني- الإسكندرية (سنة النشر غير مذكورة) ص384

الفرع الأول

مفهوم الدخول غير القانوني للنظام المعلوماتي

لما كان النظام المعلوماتي هو محل الاعتداء في جريمة الدخول غير المصرح به، فإنه من الضروري الوقوف على بيان المقصود بالنظام المعلوماتي، ثم بيان المقصود بفعل الدخول غير المصرح به، وذلك على النحو الآتي:

أولا: تعريف النظام المعلوماتي:

يعرف البعض نظام المعلومات بأنه (بيئة تحتوي على عدد من العناصر التي تتفاعل فيما بينها ومع محيطها بهدف جمع البيانات ومعالجتها حاسوبيا وإنتاج وبث المعلومات لمن يحتاجها لصناعة القرارات)[1]، ويهدف النظام المعلوماتي وفقا لهذا التعريف المتقدم إلى جمع البيانات ومعالجتها وإنتاج وبث المعلومات. ويتكون من عدة عناصر هي، اختصاصي أنظمة المعلومات أو الحاسوب ، ومنظومات حاسوب بجانبها المادي (Hardware) والبرمجيات (software)، ومنظومات الاتصال (الهواتف والتلكس والأقمار الصناعية وغيرها).

وقد عرفت المادة الأولى الفقرة (أ) من اتفاقية بوادبست المتعلقة بالجريمة الإلكترونية النظام المعلوماتي بأنه (كل آلة بمفردها أو مع غيرها من الآلات المتصلة أو المرتبطة، والتي يمكن أن تقوم سواء بمفردها أو مع مجموعة عناصر آخرى، تنفيذاً لبرنامج معين، بأداء معالجة آلية للبيانات.)، وقد فصلت المذكرة التفسيرية للاتفاقية المقصود بالنظام المعلوماتي بأنه جهاز يتألف من مكونات مادية ومكونات منطقية، وذلك بهدف المعالجة الآلية للبيانات الرقمية، ويشتمل على وسائل إدخال وآخراج وتخزين البيانات، وقد يكون هذا الجهاز منفردا أو متصلا بمجموعة من الآلات المماثلة عن طريق شبكة.[2]

---

(1) د. عماد الصابغ – نظم المعلومات (ماهيتها ومكوناتها) دار الثقافة للنشر والتوزيع- عمان- الطبعة الأولى 2000 – صـ 11

(2) د. هلالي عبداللاه - مرجع سابق – صـ41-43

وعرف نظـام مكافحة جرائم المعلوماتية السعودي لسنة 2007 في مادتـه الأولى نظام المعلومـاتي بأنـه (مجموعـة بـرامج وأدوات معـدة لمعالجـة البيانـات وإدارتهـا، وتشـمل الحاسبات الآلية)[1]

كـذلك عـرف قـانون مكافحـة جـرائم تقنيـة المعلومـات العـماني لسـنة 2011 النظـام المعلوماتي بذات التعريف الذي تبناه المشـرع السعودي حيث تنص المـادة رقـم (1) الفقـرة (ي) بأنـه (مجموعـة بـرامج وأدوات تسـتخدم في معالجـة وإدارة البيانـات والمعلومـات الإلكترونية)[2].

ويتضح لنا من التعريفـات المتقدمـة أن وظيفـة النظـام المعلومـاتي تتركـز عـلى معالجـة البيانات وإدارتها، وقد جاء بمعجم الحاسبات الصادر من مجمع اللغـة العربيـة بأنـه يقصـد بمعالجة البيانات (Data Processing) أو تشغيل البيانات (إجراء عمليات حسابية ومنطقية على البيانات لاستخراج معلومات ونتائج محددة منها)[3]

ثانيا: مفهوم الدخول غير القانوني للنظام المعلوماتي:

يقصد بالدخول غير القانوني للنظام المعلوماتي بأنه الولوج غير المصرح به أو بشـكل غـير مشـروع إلى نظام معالجة آلية للبيانات باستخدام الحاسـوب بحيـث يتحقـق الـدخول غـير المشـروع إلى النظـام المعلومـاتي بالوصـول إلى المعلومـات والبيانـات المخزنـة داخـل النظـام المعلوماتي ودون رضاء من المسئول عن هذا النظام أو المعلومات التي يحتوي عليها[4]

وقد عرف نظــام مكافحـة جـرائم المعلوماتيـة السـعودي لسـنة 2007 في مادتـه الأولى الدخول غير المشــروع بأنـه (دخـول شـخص بطريقـة متعمـدة إلى حاسـب آلي، أو موقـع إلكتروني أو نظام معلوماتي، أو شـبكة حاسـبات آليـة غـير مصرح لـذلك الشـخص بالـدخول إليها.)

---

(1) نـص هـذا القـانون منشـور عـلى الموقـع الإلكـتروني لهيئـة الاتصـالات وتقنيـة المعلومـات السـعودية www.citc.gov.sa

(2) نص هذا القانون منشور على موقع هيئة تقنية المعلومات العمانية http://www.ita.gov.om

(3) معجم الحاسبات – مجمع اللغة العربية - الطبعة الثانية الموسعة - القاهرة 1995 – صـ 56

(4) د. أيمن عبدالله فكري – مرجع سابق – صـ221

مع تقديري للتعريفين المتقدمين، فإنه يؤخذ عليهما بأنهما لم يشملا حالة الدخول المجرد دون قصد الوصول إلى المعلومات أو الحصول عليها،مثال على ذلك حالات الاختراق والدخول غير القانوني الذي يقوم به صغار السن بقصد استعراض مهاراتهم وتحدي الآخرين فقط، دون قصد الوصول إلى المعلومات إدراكاً منهم لحجم الخطأ الذي يرتكبونه، ولا تقدير لأهمية المعلومات التي قد تقع تحت أيديهم. أو حالة الدخول غير القانوني التي يقوم فيها المخترقين من هواة التحدي باختراق نظام معلوماتي معين والدخول إليه أيضاً لإثبات القدرة على الدخول والاختراق فقط دون أن يستكملوا نشاطهم بالوصول إلى المعلومات، ليس لعدولهم عن نشاطهم الإجرامي، بل لأن النشاط الذي قصدوه قد استنفذوه ونفذوه كاملاً بالحد الذي أرادوه.

ويرى آخرون بأن الدخول غير القانوني هو قيام شخص غير مرخص له بإساءة استخدام الحاسب الآلي ونظامه أو الدخول إليه بقصد الوصول إلى المعلومات والبيانات التي يحتويها الحاسب الآلي بهدف الاطلاع عليها أو لإثبات القدرة على اختراق نظم حماية المعلومات أو لأي سبب آخر.[1]

ومن جانبي أتفق مع هذا التعريف لشموله حالات الدخول غير القانوني سواء بقصد الوصول إلى المعلومات أو الدخول المجرد والذي يقوم به الفاعل لاستعراض قدرته على الاختراق، حيث أن كلا الفعلين يشكل جريمة وينتج عنهما ضررٌ للغير ويمس بسرية المعلومات الإلكترونية ويعرضها لمخاطر الإفشاء كما سنبينه لاحقاً.

---

(1) د.نائلة عادل محمد فريد قورة - مرجع سابق صـ326

الفرع الثاني

الركن المادي لجريمة الدخول غير القانوني للنظام المعلوماتي

يلزم لقيام جريمة الدخول غير القانوني للنظام المعلوماتي أن يفرغ الجاني نيته الإجرامية في انتهاك نظام معلوماتي معين غير مصرح له،بأن يقوم بالدخول إليه بقصد الوصول إلى المعلومات التي يحتويها أو بقصد ارتكاب جريمة أحرى، في نشاط خارجي أو فعل مادي يظهر من خلاله تلك النية أو الإرادة الآثمة وهو ما يمثل الركن المادي لهذه الجريمة.

أولا: وسائل الدخول غير القانوني للنظام المعلوماتي

تتناول هذه الجزئية من البحث الوسائل التي يستخدمها المجرم المعلوماتي في ارتكاب جريمته، وهو موضوع وإن كان يتسم بالفني البحت، إلا أنّ في تناوله ضرورة وفائدة عملية تتمثل، في إحاطة المشتغلين بالقانون والقضاء بالحد الأدنى من المعرفة الفنية التي تساعدهم على فهم الجريمة بشكل أعمق وأوضح.

غالبا ما يتعرض مالكوا النظم المعلوماتية والشبكات الإلكترونية لعملية الاختراق من قبل قراصنة الانترنت،ويرجع ذلك لعدة أسباب يأتي في مقدمتها غياب أو قلة الوعي أو الإهمال في تحصين نظم المعلومات والشبكات ضد مخاطر الاختراق باستخدام برامج الحماية، أو استخدام وسائل وبرامج حماية بدائية وسهلة الكسر يسهل على أي شخص على دراية بكيفية الاختراق استغلال الثغرات الموجودة بها، وبالتالي يسهل عليه الدخول والوصول إلى المعلومات المتوفرة في تلك النظم والمنقولة عبر الشبكات.

والمجرم المعلوماتي كغيره من المجرمين يلجأ إلى وسائل وأساليب مختلفة في ارتكاب جريمته، وهو في سعي مستمر إلى تطوير الوسائل المتاحة له، أو قد يلجأ إلى استحداث وسائل وأساليب جديدة، وهو ما يتواءم مع طبيعة الصراع والتنافس المستمر بين صانعي البرامج الإلكترونية والمجرم المعلوماتي والمتمثل في البحث عن الثغرات الأمنية أو خلق تلك الثغرات في البرامج الإلكترونية

والنظم المعلوماتية من قبل المجرم المعلوماتي، في مقابل السعي الدائم من جانب صانعي البرامج الإلكترونية إلى سد ومعالجة الثغرات التي يمكن أن ينفذ من خلالها المجرم المعلوماتي، وتطوير برامج الحماية اللازمة لذلك. وفيما يلي نتناول بعض الوسائل التي قد يلجأ إليها الجاني في جريمة الدخول غير القانوني للنظام المعلوماتي:

أ- في بعض الحالات قد لا يتطلب ارتكاب جريمة الدخول غير القانوني سوى قيام الجاني بضغط زر تشغيل الحاسب الآلي حتى يتمكن من الدخول إليه والتجول داخله والاطلاع على ما يحتويه من معلومات. ويتصور ذلك بالنسبة للأجهزة التي يغفل مالكوها عن تثبيت برامج الحماية أو وضع شفرة خاصة بالدخول.

ب- قد يلجأ الجاني إلى التجربة العشوائية لكلمات السر، حيث يقوم بتجريب كل القيم الممكنة للوصول إلى كلمة السر أو لكسر شفرتها، وفي الوقت الحالي توفر العديد من المواقع الإلكترونية على شبكة الانترنت برامج لكسر كلمات السر أو الشفرة، حيث تقوم تلك البرامج باستخدام كلمات القاموس والتخمين العشوائي لكسر الشفرة، ويمكن خلال عدة ساعات الحصول على كلمة السر المطلوبة.[1]

ج- استغلال الثغرات الأمنية الموجودة في النظم والشبكات والنفاذ من خلالها[2]، وتعد الأبواب الخلفية الموجودة في النظم المعلوماتية والتطبيقات

---

(1) حسن طاهر داود – مرجع سابق – صـ143

(2) في عام 2005 قام احد قراصنة الومبيوتر باختراق موقع شركة ماستركارد انترناسيونال التي أعلنت أنه تم اكتشاف هذا الخرق عبر شركة "كارد سيستمز سولوشنز" في أطلنطا المتخصصة في عمليات تحويل أموال للبنوك والتجار. وحذّرت الشركة أن بطاقات الاعتماد بكافة أنواعها قد تكون مُعرّضة. واعتبرت أن ثغرات أمنية مكّنت شخصا غير مسموح به من التسلل إلى شبكة "كارد سيستمز" وولوج معلومات صاحب بطاقة الاعتماد.

وذكرت الشركة إن 14 مبيون من زبائنها قد تعرّضوا لعمليات تزوير، فيما تعرّض 22 مليون آخرين من حاملي بطاقات "فيرا كاردز". كما ذكرت المتحدثة باسم "ماستركارد" إن المعلومات المخترقة- الأسماء، والبنوك، وأرقام الحسابات- قد تُستعمل لسرقة أموال ولكن لا يمكن استعمال هوية صاحبها. وقد أكدت شركة "كاردسيسمز سولوشن" أنها في صدد تطوير إجراءاتها الأمنية.

http://news bbc.co.uk/hi/arabic/sci_tech/newsid_4107000/4107892.stm

والبرامج من أبرز صور الثغرات الأمنية التي يستغلها الجاني لاقتحامه والوصول إلى المعلومات المخزنة فيه. والأبواب الخلفية هي عبارة عن حساب مستفيد مخبأ في النظم والتطبيقات Hidden Accounts تكون له صلاحيات مطلقة Administrator- Level Authorities تضعه الشركات المصنعة بهدف تسهيل مهمة الفنيين الذين يقدمون المساعدة الفنية للمستخدم في حالة فقدانه أو نسيانه لكلمة السر الخاصة بالنظام أو التطبيقات، وتكون كلمة السر لهذا الحساب غير قابلة للتغيير، الأمر الذي يتسبب بوجود ثغرة أمنية في النظام المعلوماتي يمكن استغلالها ممن يطلق عليهم (المخترقون - Hackers) وهذه الثغرة تكاد تكون في موجودة في أغلب أجهزة الشبكات التي يقتنيها الأفراد والشركات وحتى الجهات الأمنية.

وعلى الرغم من اتخاذ مستخدمي الأجهزة أو النظم التي تحتوي الأبواب الخلفية هذه مختلف تدابير الأمن والحماية تظل هذه النظم عرضة للاقتحام والدخول غير القانوني عن طريق تلك الأبواب الخلفية.[1]

ح- قد يلجأ الجاني إلى أسلوب انتحال شخصية أحد المستفيدين الشرعيين للحصول على كلمة السر[2]، كأن يقوم الجاني بالاتصال بأحد بالمستخدمين الشرعيين وإقناعه بأنه خادم الموقع ، ويقوم بعرض رسالة مزورة عليه يطلب

---

(1)حسن طاهر داود - مرجع سابق صـ 143 - 144

(2) في عام 2010 قام شاب بحريني بسرقة أكثر من أربعة آلاف بريد اليكتروني لفتيات صغيرات، حيث تمكن بهذه الوسيلة من سرقة صورهن الخاصة من على أجهزة الكمبيوتر الخاصة بهن، كما قام بالتقاط أفلام لهن خلسة بكاميرة الكمبيوتر بعد أن خدعهن وجعلهن يعتقدن أنه واحدة من صديقاتهن، وقد تمكن من الحصول على كلمات المرور الخاصة بالضحايا عن طريق الخدعة حيث قام بالاتصال بواسطة الانترنت على إحدى ضحاياه عن طريق برنامج (الماسنجر) منتحل شخصية صديقة لها تعرفها جيدا، فتجاوبت معها وبدأت المحادثة عادية، وخلال المحادثة طلب منها أن تتبادل معه كلمة المرور password، فأعطته كلمة المرور الخاصة بإميل آخر، نسيت أن به صورا تخصها هي وصديقتها، واكتشفت بعد ذلك سرقة هذا الإميل والصور، وأن التي تتحدث معها ليست صديقتها التي تعرفها، وإنما شخص سرق ايضا اميبها وعاد ليبتزها بنشر الصور التي سرقها على الإنترنت، إذا لم تقبل بممارسة الجنس معه. المرجع - جريدة أخبار الخليج البحرينية - العدد رقم (12441) - الأحد 23 جمادى الأولى 1433هـ- 15 أبريل 2012 - صـ 11

منه إعادة إدخال الاسم وكلمة السر، فيقدم المستخدم الضحية طائعا وهو تحت تأثير تلك الخدعة أسمه وكلمة السر للجاني، والذي بدوره يستغلها للدخول للموقع الإلكتروني أو النظام المعلوماتي المستهدف.[1]

خ- استخدام برامج متخصصة في اختراق المواقع أو الشبكات وفك الشفرات وفحص الثغرات، والتي أضحت منتشرة بكثرة على مختلف مواقع ومنتديات الانترنت، والتي تقدمها إما بأسعار زهيدة وفي كثير من الأحيان تقدمها مجاناً مع شرح مفصل لكيفية عمل البرنامج وعملية الاختراق ذاتها.[2]

ثانيا: محل الدخول غير القانوني إلى النظام المعلوماتي:

تنص المادة (2) من اتفاقية بودابست لسنة 2001 المتعلقة بالجريمة الإلكترونية على أنه (يجب على كل طرف أن يتبنى الإجراءات التشريعية أو أية إجراءات آخرى يرى أنها ضرورية من أجل اعتبارها جريمة جنائية، وفقا لقانونه الداخلي، للولوج العمدي لكل أو لجزء من جهاز الحاسب الآلي بدون حق، كما يمكن له أن يشترط أن ترتكب الجريمة من خلال انتهاك إجراءات الأمن، بنية الحصول على بيانات الحاسب أو أية نية إجرامية آخرى، أو أن ترتكب الجريمة في حاسب آلي يكون متصلاً عن بعد بحاسب آخر)

---

(1) حسن طاهر داود - مرجع سابق- صـ 145

(2) فيما يلي نسرد بعض الأمثلة على برامج الاختراق وفك الشفرات :

أ) **برنامج Kismet** : يقوم هذا البرنامج بإظهار الشبكة والماك أدرس لراوتر Kismet .ويعطي المستخدم معلومات عن الأجهزة المستخدمة في الشبكة وعن أنواع التشفير المستخدمة وإذا كانت الشبكة فيها ثغر أو لا بحيث يتمكن من اختراقها.

ب) **برنامجWIFI-Radar** : يقوم هذه البرنامج بعمل مسح للشبكات اللاسلكية، ويمكن مستخدمه من إنشاء ملف خاص لكل شبكة، واختيار طريقة الاتصال بهم، ويخزن إعدادات كل شبكة.

ج) **برنامج Air Snort**:هو عبارة عن برنامج مخصص لكسر التشفير من نوع..WEP

د) **برنامج Air Crack** يعمل هذا البرنامج بنفس طريقة البرنامج السابق ولكنه يمتاز بأنه أكثر كفاءة منه، ولهذا البرنامج عدة أنواع وهي:

- Airodump : يقوم بجمع الرزم اللازمة لغايات كسر الشفرة
- Airdecap: يقوم بفك تشفير الرزم المكتشفة
- Aircrac: البرنامج الرئيسي والذي يقوم بتحليل المعلومات من الرزم المجموعة ويقوم بفك تشفيرها

هـ) **برنامج: COWPAtty** : يستخدم هذا البرنامج لفك تشفير WPA ،ويستخدم هذا البرنامج Brute-Force ويحتاج إلى عدد 4 رزم فقط ليبدأ بفك الشفرة.

وقد بينت المذكرة التفسيرية للاتفاقية في تعليقها على هذه المادة، أن الدخول أو الولوج غير القانوني (الاختراق) الذي يحدث للنظام بأكمله أو لجزء منه أياً كان، كأن يتم الدخول إلى أحد الكيانات المادية أو المعنوية مثل البرامج ، أو بيانات مخزنة في نظام التنصيب، أو بيانات تتعلق بالمرور والمحتوى، ومع ذلك فإن الدخول غير القانوني لا يشمل مجرد إرسال الرسائل الإلكترونية أو الملفات للنظام. ويشمل الدخول غير القانوني الاختراق الذي يحدث لنظام معلوماتي متصل بشبكات اتصال عامة أو لنظام معلوماتي متصل بذات الشبكة، أي شبكة محلية أو دولية (انترنت) أو أي شبكة خاصة لشركة أو مؤسسة، وعلى أية حال، فإن طريقة الاتصال لا تدخل في الاعتبار سواء أكانت عن بعد أم كانت في نطاق قريب[1].

يلاحظ مما تقدم أن اتفاقية بودابست لم تفرض أسلوباً محدداً لتجريم الدخول غير القانوني وإنما تركت الخيار للدول الموقعة على الاتفاقية تبني ما تراه مناسباً من إجراءات لتجريم هذا الفعل، وفي تحديد محل الدخول غير القانوني سواء لكل أو لجزء من نظام الحاسب الآلي وسواء كان النظام المعلوماتي متصل بشبكات اتصال عامة أو متصل بذات الشبكة، أي شبكة محلية أو دولية (انترنت) أو أية شبكة خاصة لشركة أو مؤسسة.

ولقد تأثرت العديد من التشريعات بالمادة السابقة ولاسيما الدول الموقعة على تلك الاتفاقية، حيث نلاحظ أن بعض التشريعات تجرم الدخول غير القانوني إلى كل أنظمة الحاسبات الآلية و شبكات المعلومات وما يترتب على ذلك تجريم عمليات الاعتراض غير المشروعة للاتصالات التي تتم من خلال الدخول إلى هذه الشبكات وأبرز مثال على ذلك قانون العقوبات الفرنسي الذي يجرم في مادته 1/321 فعل الدخول أو البقاء غير المشروع داخل نظم المعالجة الآلية للمعلومات بالمعنى الواسع للكلمة.[2] حيث يقصد بنظام المعالجة الآلية

---

(1) د. هلالي عبدالله احمد – مرجع سابق صـ 68- 72

(2) د.نائلة عادل محمد فريد قورة – مرجع سابق صـ333

للمعلومات وفقا للتعريف الذي وضعه البرلمان الفرنسي خلال الأعمال التحضيرية للقانون بأنه (مجموعة وحدات المعالجة أو الذاكرة أو البيانات أو نظام الدخول أو الخروج أو وحدات الاتصال التي تساعد على تحقيق النتيجة المطلوبة وتكون موضوعة للحماية بنظام الأمن)[1]، ويترتب على هذا التوسع في تعريف نظم المعالجة الآلية أن التقاط الإشارات الناجمة عن عملية تبادل المعلومات من خلال الشبكات تعد دخولا غير مصرح به إلى نظام المعالجة الآلية الذي يحتوي على هذه المعلومات. وأخذ بذات الاتجاه القانون الفيدرالي الأمريكي الخاص بإساءة استخدام الحاسبات الآلية حيث تجرم المادة 1030 (a) (2) الحصول على المعلومات عن طريق الدخول غير القانون إلى الحاسبات الآلية، وتجرم المادة 1030 (a) (3)[2] الدخول المجرد إلى الحاسبات

---

(1) د. أيمن عبدالله فكري - مرجع سابق - صـ223

(2) USA Computer Crimes Acts 18 U.S.C. 1029.(**1030**. Fraud and Related Activity in Connection with Computers

(a) Whoever

(1) having knowingly accessed a computer without authorization or exceeding authorized access, and by means of such conduct having obtained information that has been determined by the United States Government pursuant to an Executive order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data, as defined in paragraph y. of section 11 of the Atomic Energy Act of 1954, with reason to believe that such information so obtained could be used to the injury of the United States, or to the advantage of any foreign nation willfully communicates, delivers, transmits, or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it;

(2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains--

(A) information contained in a financial record of a financial institution, or of a card issuer as defined in section 1602(n) of title 15, or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.);

(B) information from any department or agency of the United States; or

(C) information from any protected computer if the conduct involved an interstate or foreign communication;

(3) intentionally, without authorization to access any nonpublic computer of a department or agency of the United States, accesses such a computer of that department or agency that is exclusively for the use of the Government of the United States or, in the case of a computer not exclusively for such use, is used by or for the Government of the United

الآلية الخاصة بالحكومة الأمريكية، أو إلى الحاسبات التي يؤدي الدخول غير القانوني إليها المساس بأعمال تتعلق بالحكومة الأمريكية، والحاسبات الآلية تشتمل وفقا لهذا القانون على كل جهاز الكتروني أو كيميائي أو كهربائي أو جهاز سريع لمعالجة المعلومات وكذلك وسائل الاتصالات التي تعمل بالاتصال مع أي من هذه الأجهزة. ومن الدول التي أخذت بهذا الاتجاه الواسع أيضا كل من اليونان والنرويج وفنلندا [1]

وبمطالعتنا موقف التشريعات العربية لاحظنا أن بعض هذه التشريعات أخذت بالاتجاه السابق مثل قانون مكافحة جرائم تقنية المعلومات العماني لسنة 2011 الذي جرم الدخول غير القانوني إلى موقع الكتروني أو نظام معلوماتي أو وسائل تقنية المعلومات، ونص صراحة على تجريم الدخول إلى كل أو جزء مما سبق ذكره، حيث تنص المادة الثالثة من هذا القانون على أنه (يعاقب بالسجن مدة لا تقل عن شهر ولا تزيد على ستة أشهر وبغرامة لا تقل عن مائة ريال عُمانى ولا تزيد على خمسمائة ريال عُمانى أو بإحدى هاتين العقوبتين ، كل من دخل عمدا ودون وجه حق موقعا إلكترونيا أو نظاما معلوماتيا أو وسائل تقنية المعلومات أو جزءا منها أو تجاوز الدخول المصرح به إليها أو استمر فيها بعد علمه بذلك..). وبمراجعة المادة الأولى من هذا القانون الخاصة نجد أنها تعرف النظام المعلوماتي بأنه مجموعة برامج وأدوات تستخدم في معالجة وإدارة البيانات والمعلومات الإلكترونية.أما الموقع الإلكتروني فهو مكان إتاحة المعلومات الإلكترونية على الشبكة المعلوماتية من خلال عنوان محدد. وتعرف وسيلة تقنية المعلومات بأنها جهاز الكتروني يستخدم لمعالجة البيانات والمعلومات الإلكترونية أو تخزينها أو إرسالها أو استقبالها كأجهزة الحاسب الآلي وأجهزة الاتصال.).وبذات الاتجاه أخذ أيضاً نظام مكافحة جرائم المعلوماتية السعودي لسنة 2007 حيث تعرف الفقرة (7) من المادة الأولى منه الدخول غير المشروع بأنه (دخول شخص بطريقة متعمدة إلى حاسب آلي، أو موقع إلكتروني أو نظام

States and such conduct affects that use by or for the Government of the United States...)
http://www.law.cornell.edu/uscode/18/1030.html

(1) د.نائلة عادل محمد فريد قورة – مرجع سابق صـ334 - 335

معلوماتي، أو شبكة حاسبات آلية غير مصرح لذلك الشخص بالدخول إليها.....)

بينما تتجه بعض التشريعات الآخرى إلى تجريم الدخول غير القانوني إلى البرامج والمعلومات التي يحتوي عليها الحاسب الآلي مستبعدة شبكات المعلومات مثال ذلك قانون إساءة استخدام الحاسبات الآلية الانجليزي لسنة 1990 حيث تعاقب المادة الأولى منه على الدخول غير القانوني إلى البرامج والمعلومات التي يحتوي عليها أي حاسب آلي، ولم تتضمن هذه المادة أي إشارة إلى شبكات المعلومات.(1) وبمراجعتنا موقف التشريعات العربية نلاحظ أن قانون مكافحة جرائم تقنية المعلومات الإماراتي لسنة 2006 أخذ بهذا الاتجاه حيث جرم في مادته الثانية الفقرة (1) الدخول غير القانوني إلى الموقع الإلكتروني أو نظام معلوماتي دون الإشارة إلى شبكات المعلومات، حيث تنص تلك المادة على أنه (1- كل فعل عمدي يتوصل فيه بغير وجه حق إلى موقع أو نظام معلوماتي سواء بدخول الموقع أو النظام أو بتجاوز مدخل مصرح به، يعاقب عليه بالحبس وبالغرامة أو بإحدى هاتين العقوبتين.)

كما سبق الإشارة إلى أن المادة الثانية من اتفاقية بودابست المتعلقة بالجريمة الإلكترونية تركت الخيار للدول لاختيار الأسلوب الأنسب لها لتجريم الدخول غير القانوني ومن بين تلك الأساليب أن يمكن اشتراط أن ترتكب الجريمة في حاسب آلي يكون متصلاً عن بعد بحاسب آخر، فقد أخذ بهذا الاتجاه قانون العقوبات السويسري المعدل عام 1995 في المادة (143) مكرر التي تجرم الدخول غير القانوني إلى أنظمة الحاسبات الآلية بواسطة جهاز لنقل المعلومات حيث يتناول هذا النص حالات الدخول غير القانوني إلى النظام المعلوماتي التي

---

(1) المرجع نفسه – صـ 336 ، نص المادة باللغة الانجليزية :

COMPUTER MISUSE ACT 1990 (UK) (1.(1) A person is guilty of an offence if -

(a) he causes a computer to perform any function with intent to secure access to any program or data held in any computer;

(b) the access he intends to secure is unauthorised; and

(c) he knows at the time when he causes the computer to perform the function that that is the case.)

المرجع: **http://www.legislation.gov.uk/ukpga/1990/18/enacted**

يقوم بها أشخاص خارج المؤسسة التي تحتوي هذا النظام عن طريق شبكات لاتصال، وكذلك حالات الدخول غير القانوني التي تقع من العاملون داخل المؤسسة عن طريق شبكة الاتصال الداخلية. وبهذا أخذ أيضا قانون العقوبات الاسترالي في المادة 76 منه [1].

ثالثا: حالات الدخول غير القانوني إلى النظام المعلوماتي:

بعد استعراض وسائل الدخول غير القانوني إلى النظام المعلوماتي وبيان محله، نتناول في هذا البند حالات الدخول غير القانوني على النحو الآتي.

1- حالة عدم وجود سند قانوني للدخول إلى النظام المعلوماتي، وتتحقق هذه الحالة، في فرضين هما :

أ- قيام شخص غير مالك النظام المعلوماتي أو مستخدمه الشرعي، بالدخول إلى النظام المعلوماتي على غير رضاه ودون الحصول على تصريح منه

ب- دخول غير مالك النظام المعلوماتي أو مستخدمه الشرعي دون الحصول على إذن من السلطة المختصة، على سبيل المثال الحصول على إذن من النيابة العامة بالتفتيش في الحالات المنصوص عليها قانوناً، ويستفاد ذلك من العبارة التي استخدمتها معظم التشريعات (الولوج العمدي لكل أو لجزء من جهاز الحاسب الآلي بدون وجه حق)

ويلاحظ بأنه إذا كان الفرض الثاني لا يثير إشكالية عملية لأن حالات التفتيش يكون منصوصاً عليها ومحددة بالقانون وكذلك الجهة التي تصدر الإذن والأشخاص المكلفين بالتنفيذ.فإن الفرض الأول يتطلب للتحقق من وقوعه تحديد مالك النظام المعلوماتي أو من له سلطة عليه ومن يملك صلاحية إعطاء التصريح أو المستخدم الشرعي أو المصرح له بالدخول للنظام المعلوماتي ونطاق هذا التصريح .

ويقصد بمالك النظام المعلوماتي كل شخص طبيعي أو معنوي له كافة

---

(1) د.نائلة عادل محمد فريد قورة – مرجع سابق صـ338

السلطات الممكنة على النظام المعلوماتي بحيث يحق له استعماله واستغلاله والتصرف فيه. وهذا التعريف مستمد من تعريف حق الملكية باعتبار أن النظام المعلوماتي في حقيقته شيء يرد عليه حق الملكية. وقد يكون مالك النظام المعلوماتي شخص طبيعي ، أو معنوي كالمؤسسات والشركات والهيئات، والدول.أما المستخدم الشرعي أو المرخص له، فهو كل من منحه مالك النظام الرخصة لاستخدام النظام المعلوماتي إما بحكم عمله لديه أو نظير مقابل مادي. وعليه يمكننا القول بأن دخول أي شخص من خارج هذه الطائفة دون تصريح منهم أو رضائهم، أو بدون سند من القانون، فإن يكون قد أتى بالركن المادي من جريمة الدخول غير القانوني للنظام المعلوماتي.

2- حالة تجاوز التصريح أو الإذن بالدخول إلى النظام المعلوماتي:

تستنتج هذه الحالة من بعض التشريعات التي استخدمت عبارات (أو تجاوز مدخلاً مصرحاً به)[1] ، فقد يكون للشخص الداخل إلى النظام المعلوماتي سواء من داخل المؤسسة التي تحتوي على النظام المعلوماتي أو من خارجها، صلاحيات محددة وفقا لطبيعة عمله أو لطبيعة التصريح أو الأذن الممنوح له، إلا أنه يطمع في الحصول على صلاحيات أعلى من تلك الممنوحة له، أو الذهاب إلى مناطق أبعد من تلك المحددة له داخل النظام، فيلجأ إلى وسائل تمكنه من استغلال ثغرات في النظام المعلوماتي تمكنه من تحقيق أهدافه.

وعليه فإنه يعد دخولا غير قانوني، تجاوز شخص مسموح له بالدخول إلى منطقة معينة من النظام المعلوماتي،إلى مناطق آخرى غير مصرح له بالدخول إليها، وعلة ذلك أنه إذا كان التصريح يخول المصرح له حق الاطلاع على معلومات أو بيانات محددة، فإن ما عدا ذلك من معلومات وبيانات لم يرد عليها التصريح بالدخول والاطلاع عليها

---

(1) المادة الثالثة من قانون مكافحة جرائم تقنية المعلومات العماني لسنة 2011، والمادة الثانية من قانون مكافحة جرائم تقنية المعلومات الاماراتي لسنة 2006

يسـري عليهـا الأصـل العـام وهـو سـرية المعلومـات وعـدم جـواز الاطـلاع عليهـا إلا بـتصريح أو برضـاء مـن لـه سـلطة عـلى النظـام المعلومـاتي. وفي هـذه الحالـة فإنـه يتعـين أن يكـون هنـاك تحديـدٌ مسـبقٌ لـتصريح الـدخول إلى النظـام المعلومـاتي بمعنـى أن يحـدد اختصـاص كـل عامـل بالنظـام المعلومـاتي وحـدود اختصاصـه بحيـث إذا مـا تخطـى حـدود اختصاصـه شـكل فعلـه جريمـة دخـول غـير مشـروع للجـزء غـير المصرح له بالدخول إليه.

كما يشترط أن يكون الشخص مخولا بحكم القانون بالدخول إلى النظـام المعلومـاتي كـما هو الحال بالنسبة لجهة ما يمنحها القانون سلطة الرقابة على النظم المعلوماتية للتحقق من مدى مطابقتها للقوانين واللوائح المنظمة لعمل النظام المعلوماتي[1].

3- البقاء غير المصرح به داخل نظام الحاسب الآلي:

قد يفاجأ شخص ما أثنـاء اسـتخدامه للنظـام المعلومـاتي أو الحاسـب الآلي أو الشـبكة الدولية (الانترنت) بأنه قد دخل إلى نظام معلوماتي غير مصرح لـه بالـدخول إليـه أو أنـه دخل إلى جزء أو منطقة غير المرخص لـه بالـدخول إليهـا دون أن يقصـد ذلـك. وفي هـذه الحالة يكون الشخص أمـام خيـارين الأول الخـروج فـور اكتشـافه بـأمر دخولـه الخـاطئ. والثاني هو البقاء داخل النظام على الرغم من علمه بأنه غير مصـرح له بدخوله. فإذا أخذ بالخيار الأول فلا تثريب عليه. أما إذا أخذ بالخيار الثاني ففي هـذه الحالـة يسـتوي فعلـه مع فعل الدخول غير المصرح به، إذ أن اتجاه إرادة الفاعل إلى الاسـتمرار في البقـاء داخـل النظام وهو عالم أنه غير مصـرح له بدخوله ابتداءً لا تختلف عن إرادة الفاعل في الـدخول غـير المصـرح بـه. فالنتيجـة الإجراميـة واحـدة وهـي الوصـول إلى نظـام غـير مصرح له بالدخول إليه المصلحة التي يحميها القانون والمتمثلة في حماية نظام الحاسـب الآلي[2].

---

(1) د. أيمن عبدالـلـه فكري - مرجع سابق - صـ230

(2) د.نائلة عادل محمد فريد قورة - مرجع سابق صـ358

وهذا ما أخذ به قانون العقوبات الفرنسي في المادة ذ/1 الذي يعاقب على (الدخول بطريق الغش أو التدليس على نظام لمعالجة البيانات أو إبقاء الاتصال بطريقة غير مشروعة بالحبس لمدة...)[1]

وفي تقديري، يعد العقاب على البقاء الذي يلي مباشرة النفاذ قد يكون فيه إجحاف بمن ينفذ إلى النظام المعلوماتي دون قصد ، لذلك يستوجب حتى تتحقق تلك الحالة البقاء بالنظام مدة تتجاوز المدة المسموح بها للخروج منه بعد أن يكون الفاعل قد تنبه لدخوله غير المشروع ، وهي مسألة يعود تقديرها لقاضي الموضوع وفقا لظروف الواقعة.

رابعا: اشتراط اختراق إجراءات حماية النظام المعلوماتي ضد الدخول غير القانوني:

مع تزايد المخاطر التي تتعرض لها المعلومات والبيانات الإلكترونية بات من الضروري وجود نظام لحماية المعلومات والبيانات الإلكترونية من تلك المخاطر التي تهددها سواء كانت هذه المخاطر داخلية أو خارجية، لذا تتخذ معظم الجهات والأفراد تدابير وإجراءات لمنع وصول المعلومات إلى أيدي أشخاص غير مخولين بالاطلاع عليها.

ولقد آثار مدى لزوم اشتراط اختراق إجراءات حماية النظام المعلوماتي ضد الدخول غير القانوني للعقاب على الدخول غير المصرح به خلافا بين الفقهاء، حيث يذهب جانب من الفقه[2] وخاصة في فرنسا إلى عدم لزوم اشتراط وجود إجراءات حماية للنظام المعلوماتي لتحقق جريمة الدخول غير القانوني والعقاب عليها، ويستند أنصار هذا الرأي إلى أن نصوص المادتين 2/462 و 1/323 المعدلة لها من قانون العقوبات الفرنسي[3] لم تشترطا مثل هذا الشرط في جريمة

---

(1) د. أيمن عبدالله فكري – مرجع سابق – صـ218

(2) بلال أمين زين الدين – جرائم نظم المعالجة الآلية للبيانات في التشريع المقارن والشريعة الإسلامية – دار الفكر الجامعي - الإسكندرية 2008 – صـ 265 – 266

(3) تنص المادة 2/462 على أن (كل شخص قام بالدخول أو البقاء بطريقة كلية أو جزئية داخل نظام لمعالجة المعومات سيعاقب بالحبس الذي لا يقل عن شهرين ولا يزيد عن سنة وبغرامة تتراوح بين

الدخول غير القانوني والبقاء غير القانوني في النظام المعلوماتي، بالإضافة إلى أنهم يستندوا إلى الأعمال التحضيرية التي سبقت صدور قانون العقوبات الفرنسي الجديد الصادر في عام 1988 التي انتهت إلى عدم الأخذ بوجهة النظر التي كانت تنادي باشتراط شمول النظام المعلوماتي بأي من نظم الحماية، إذ كان هناك توجه لمجلس الشيوخ الفرنسي لتبني شرط وجود نظام الأمان في جريمة الدخول غير القانوني إلا أن الجمعية الوطنية الفرنسية لم تأخذ به[1].

بينما يذهب جانب آخر من الفقه إلى ضرورة اشتراط وجود نظام الحماية للنظام المعلوماتي، ويبرروا ذلك بان هذا الشرط مهم بالنسبة لشركات التأمين والتي تضع حد أدنى من الحماية الذي لا يمكن النزول عنه من قبل مستخدمي النظام المعلوماتي،حيث إن أي تقصير في تلك الحماية يؤدي إلى تحمل شركات التامين خسائر فادحة نتيجة لتحملها تعويضات ضخمة من جراء المطالبات القضائية التي تتعلق بتعويض الخسائر الناجمة عن الاعتداء على الأنظمة المعلوماتية، وأنه كان أولى بالقانون إن يعطي حماية أكبر من تلك التي توليها شركات التأمين للأنظمة المعلوماتية باشتراط أن تكون هذه النظم مشمولة بالحماية من قبل مالكيها أو مستخدميها ضد أي اعتداء قد تتعرض له مثل الاختراق والدخول غير المشروع. لذا كان على القانون أن يلزم مستخدمي أو

30000 إلى 50000 فرنك أو بإحدى هاتين العقوبتين كل من دخل بطريق الغش أو مكث عدراً في نظام لمعالجة الآلية للمعلومات أو في جزء منه. فإذا نجم عن ذلك إلغاء أو تعديل للمعلومات التي يحتويها ذلك النظام، كإتلاف عمل ذلك النظام فإن العقوبة تكون الحبس من شهرين إلى عامين والغرامة من 10آلاف إلى 100 ألف فرنك)

- وفي عام 1994 صدر قانون العقوبات الفرنسي الجديد وتم إحلال المادة 1/323 مكان المادة 2/462 ، وبموجب المادة الحديدة شددت العقوبة حيث أصبحت سنة حبس ومائة ألف فرنك كغرامة ، وفي حالة ما إذا نتج عن هذا الدخول غير المشروع محو أو تعديل في المعلومات الموجودة بالنظام تكون العقوبة الحبس سنتين ومائتين ألف فرنك فرنسي كغرامة.

وفي 2004 شدد المشرع الفرنسي العقوبة المقررة بخصوص هذه المادة فجعلها سنتين حبس و15 ألف يورو (العمة الأوروبية الموحدة) ، وفي حالة ما إذا نتج عن هذا الدخول غير المشروع محو أو تعديل في المعلومات الموجودة بالنظام تكون العقوبة الحبس ثلاث سنوات وثلاثين ألف يورو كغرامة- راجع د. عمر أبو الفتوح عبدالعظيم الحمامي – مرجع سابق – صـ865 - 866

(1) حيث كان مجلس الشيوخ الفرنسي يتمسك بهذا الشرط وكانت حجته في ذلك جذب انتباه أصحاب الأنظمة إلى هذه النقطة الأساسية كي يدعموا أنظمتهم بأجهزة الحماية، في حين رأت الجمعية الوطنية أنه من غير المناسب التمسك بهذا الشرط ، لأنه سيترتب عليه قصر الحماية الجنائية على نظم المعلومات المحمية بواسطة نظم حماية وبالتالي استبعاد من مجال تطبيق النص أفعال الدخول غير القانوني التي ترتكب ضد الأنظمة المفتوحة للعامة، - د. محمد سامي الشوا - مرجع سابق – صـ209 - 210

مالكي النظم المعلوماتية باتخاذ إي من تدابير الحماية للأنظمة التابعة لهم بالقدر التي تتناسب مع أهمية وسرية ما تحتويه تلك النظم من معلومات أو بيانات. كما يرى أنصار هذا الاتجاه عدم جدارة معلومات لو كانت ذات أهمية بالحماية تركها المسئولون عنها دون أي إجراءات تكفل حمايتها. حيث إن النظم المعلوماتية بطبيعتها منفتحة ومرتبطة بالخارج من خلال اتصالها بشبكات المعلومات وهو ما يجعلها أكثر عرضة لخطر الاعتداء من قبل المخترقين والمتطفلين ونظرا لأهمية المعلومات أو البيانات التي قد تحتوي عليها، والمخاطر التي قد تتعرض لها فإنه بات من الضروري توفير الحماية اللازمة لها من قبل المسئولين عنها. ويستند أنصار هذا الاتجاه إلى المادة (28) من القانون رقم 78 – 17 لعام 1978 الخاص بالمعلوماتية وحماية الحريات، والتي تتطلب ضرورة اتخاذ تدابير أمنية لحماية نظم المعلومات ضد أي تلاعب أو إتلاف أو الدخول غير القانوني، وبالتالي فلا مبرر للتفرقة بين المعلومات والبيانات الشخصية التي يحميها هذا القانون وبين غيرها من المعلومات الإلكترونية التي تحميها المادة 232- 1 من قانون العقوبات الفرنسي.[1]

ويرى البعض الآخر ضرورة وجود نظام أمني لقيام الجريمة خاصة أن اختراق هذه الحماية الفنية والأمنية والدخول إلى نظام المعالجة الآلية يشكل دليلا قاطعا على توفر ركن العمد لدى الجاني، حيث لا يمكن تصور أن يكون دخوله للنظام المعتدى عليه محض صدفة، وقد استعمل طرق تقنية معقدة لخرق هذه الحماية[2].

وعلى الرغم من وجاهة الحجج التي ساقها أنصار الاتجاه الذي يتطلب اشتراط توافر نظام حماية للناظم المعلوماتي، إلا إننا نميل إلى الاتجاه الذي يذهب إلى بسط الحماية الجنائية لنظم المعلومات بغض النظر عن تمتعها بنظام حماية من عدمه، ذلك أن قصرالحماية الجنائية على النظم المعلوماتية التي يوفر لها

---

(1) د.نائلة عادل محمد فريد قورة – مرجع سابق صـ366- 367

(2) عبدالفتاح بيومي حجازي، النظام القانوني لحماية التجارة الالكترونية: الكتاب الثاني، الحماية الجنائية للتجارة الالكترونية، دار الفكر الجامعي الإسكندرية 2002، ص 24.

مالكوها نظم حماية ويشملوها بتدابير أمنية، يؤدي إلى إفلات بعض المجرمين الذين يقومون بالاعتداء على خصوصية وسرية معلومات الآخرين من العقاب لمجرد كون النظم المعلوماتية التي وقع عليها الاعتداء غير مؤمنة بما يكفي من قبل مالكيها، وهو في حقيقته يشكل عقاباً غير مباشر لمالكي تلك النظم المعتدى عليها، وخاصة إذا لم يكن هناك التزام قانوني يلزمه بوضع برامج أو اتخاذ تدابير محددة لحماية النظام المعلوماتي، وحتى لو كان هناك مثل هذا الالتزام، فإن ذلك لا يعني عدم مجازاة المعتدي على حرمة النظام المعلوماتي نتيجة لإخلال المعتدى عليه بقواعد الحماية. وندعم رأينا هذا، بأنه في جريمة السرقة لا يؤثر تمتع المال المسروق بنوع معين من الحماية من قبل مالكه من عدمه على قيام جريمة السرقة، ذلك أن التشريعات توفر الحماية للمال الضائع وتعاقب من يستولي عليه بنية تملكه مثال مادة (396) من قانون العقوبات البحريني لسنة 1976 التي تنص على أنه (يعاقب بالحبس مدة لا تزيد على سنتين أو بالغرامة التي لا تجاوز مائتي دينار من استولى بنية التملك على مال ضائع أو على مال وقع في حيازته غلطا أو بقوة قاهرة .)، وعليه فإنه من باب أولى حماية النظم المعلوماتية بغض النظر عن مدى تمتعها بنظام حماية أمنية من عدمه، إذ أن علة التجريم متوفرة في الحالتين وهي حماية سرية خصوصية المعلومات.

والاختلاف حول اشتراط تمتع النظم المعلوماتية بنظم حماية أمنية لم يقتصر على الفقه فحسب، بل امتد أيضا إلى التشريعات، حيث لم تأخذ بعض التشريعات بهذا الشرط مثل قانون العقوبات الفرنسي والإنجليزي والسويدي، بينما تطلبت بعض التشريعات لقيام جريمة الدخول غير المصرح به شروطاً تتعلق بالتدابير الأمنية، مثل القانون النرويجي والألماني والهولندي. فضلاً عن أن منظمة التعاون الاقتصادي والتنمية قد أوصت في عام 1986 بتجريم الدخول غير القانوني إلى نظام الحاسب الآلي مؤكدة على أن يكون التجريم في الحالات التي تكون الأنظمة محل الاعتداء محمية بواسطة تدابير أمنية وذلك بما يتفق مع السياسة التشريعية للدولة.[1]

---

(1) د.نائلة عادل محمد فريد قورة – مرجع سابق صـ268- 373

خامسا: النتيجة:

هل تتحقق النتيجة الإجرامية بمجرد الدخول إلى النظام المعلوماتي بصرف النظر عن الوصول إلى المعلومات المخزنة داخله؟ أم أنه يجب الوصول إلى المعلومات التي يحتويها النظام المعتدى عليه؟

تختلف الإجابة على هذا السؤال تبعا لاختلاف موقف التشريعات من جريمة الدخول غير القانوني، فقد ذهبت تشريعات إلى الاكتفاء بمجرد الدخول إلى النظام المعلوماتي كأن يقوم شخصٌ ما بتشغيل جهاز الحاسب الآلي والتجول داخله، أو تمكنه من كسر برامج الحماية ورموز التشفير الخاصة بالحاسب الآلي أو الشبكات والوصول إلى مناطق داخل النظام المعلوماتي على النحو الذي يمكنه التجول داخل النظام المعلوماتي ، سواء نجح الجاني في الوصول إلى المعلومات أو البرامج المخزنة داخل النظام محل الجريمة أم لا، ومرد ذلك في تقديري إلى أن العلة من تجريم الدخول غير القانوني هي حماية المعلومات من الوصول إليها والمساس بسلامتها، كون هذه الجريمة من الجرائم التي تمثل عدوانا محتملا على الحق المحمي.

ويأتي القانون الخاص بحماية المعلومات في السويد الصادر عام 1973 في مقدمة التشريعات التي جرمت الدخول المجرد إلى نظام الحاسب الآلي، ثم تلته في ذلك تشريعات آخرى من أوروبا مثل القانون الفرنسي والبرتغالي والهولندي والفنلندي[1].

ومن التشريعات العربية، قانون مكافحة جرائم تقنية المعلومات العماني لسنة 2011، قانون مكافحة جرائم تقنية المعلومات الإماراتي لسنة 2006، وكذلك قانون العقوبات الجزائري (المادة 394 مكرر)[2].

---

(1) المرجع نفسه صـ372

(2) في 10 نوفمبر 2004 تم إضافة قسم سابع مكرر بعنوان (المساس بأنظمة المعالجة الآلية للمعطيات) إلى الفصل الثالث من الباب الثاني من قانون العقوبات الجزائري و تنص المادة 394 مكرر على انه (يعاقب بالحبس من ثلاثة (3) أشهر إلى سنة (1) وبغرامة من 50.000 د ج إلى 100.000 د ج كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك...) راجع - http://www.joradp.dz/TRV/APenal.pdf

هذا وقد ذهبت تشريعات آخرى إلى اشتراط أن يتم الوصول إلى المعلومات التي يتضمنها النظام المعلوماتي للقول بتحقق الدخول غير القانوني إلى النظام المعلوماتي، مثال القانون الفيدرالي الأمريكي لجرائم الحاسبات الآلية المادة 1030(a) (1) ، (2) الذي لا يعاقب على الدخول المجرد إلى النظام المعلوماتي بل يتطلب الحصول على المعلومات، إلا أنه يجرم في المادة 1030 (a) (3)مجرد الدخول بالنسبة للحاسبات الآلية التي تعمل داخل الحكومة الفدرالية أو تلك التي لا تعمل داخل الحكومة الفدرالية ولكن من شأن الدخول غير القانوني إليها التأثير على مصالح الحكومة التي ترتبط بأي صورة بتلك الحواسيب[1].

وبمطالعة التشريعات العربية نلاحظ أن نظام مكافحة جرائم المعلوماتية السعودي لسنة 2007، أخذ بذات الاتجاه، حيث جرم الدخول غير المشروع بالمواد 3-5-7 إلا أنه اشترط أن يكون الدخول غير المشروع لتهديد شخص أو ابتزازه لحمله على القيام بفعل أو الامتناع عنه, أو الدخول غير المشروع إلى موقع إلكتروني، أو الدخول إلى موقع الكتروني لتغيير تصاميم هذا الموقع، أو إتلافه، أو تعديله، أو شغل عنوانه ، بالإضافة إلى الدخول غير المشروع لإلغاء بيانات خاصة، أو حذفها، أو تدميرها، أو تسريبها، أو إتلافها أو تغييرها، أو إعادة نشرها أو الدخول غير المشروع إلى مواقع الكترونية أو نظم معلوماتية أو أحد أجهزة الحاسب الآلي للحصول على البيانات التي تتعلق بأمن الدولة أو اقتصادها.

ومن جانبي أرجح الاتجاه الذي يجرم مجرد الدخول غير المشروع والمعاقبة عليه بغض النظر عن وصول الجاني إلى المعلومات أو البرامج من عدمه، مع تشديد العقوبة تبعا لطبيعة النظام المعلوماتي والمعلومات التي يحتوي عليها وطبيعة العلاقة بين الجاني والنظام المعلوماتي. ذلك أن مجرد الدخول غير القانوني يعد انتهاكاً لحق الغير في خصوصية معلوماته الإلكترونية، كما يعد الشرارة

---

(1) نص المادة منشور على الموقع الإلكتروني

http://www.law.cornell.edu/uscode/18/1030.html

الأولى أو البوابة لارتكاب جرائم معلوماتية أكثر خطورة وجسامة. فضلا عما يترتب عليه من خسائر مادية كبيرة للمجني عليه نظرا لما يتطلبه وقف هذا الدخول من جهود ونفقات مالية.

ومن زاوية آخرى لو فرضنا أن شخصا ما تمكن من الدخول بطريقة غير مشروعة واكتفى بهذا الدخول ولم يصل إلى المعلومات كمن أراد إثبات القدرة على الاختراق وتحدي نظم الحماية، فإنه في هذه الحالة وإن لم يصل أو يعبث بالمعلومات المخزنة داخل النظام المعلوماتي، فإنه وهو في طريقه للدخول قد أتلف أو دمر برامج حماية النظام المعلوماتي، وأحدث ثغرات في النظام المعلوماتي من شأنها تسهيل مهمة غيره من المخترقين في اختراق هذا النظام المعلوماتي بالنفاذ من خلال تلك الثغرات والوصول إلى المعلومات المخزنة داخله.

ويمكن قبول تأسيس الفكرة المتقدمة على جريمة دخول مكان مسكون أو معدٍ للسكن أو محل معدٍ لحفظ المال أو عقارا خلافا لإرادة صاحب الشأن وفي غير الأحوال المبينة بصورة مجردة، بحيث تتحقق الجريمة بمجرد الدخول ولو لم يعرف قصد الفاعل من الدخول (المادة 361) من قانون العقوبات البحريني لسنة 1976.

الفرع الثالث

الركن المعنوي لجريمة الدخول غير القانوني للنظام المعلوماتي

لا يكفي لتقرير المسؤولية الجنائية أن يصدر عن الجاني سلوك إجرامي ذو مظهر مادي بل لابد من توافر ركن معنوي وهو عبارة عن النية الداخلية أو الباطنية التي يضمرها الجاني في نفسه.

وتعد جريمة الدخول والبقاء غير القانونين في النظام المعلوماتي وفقا لما ذهبت إليه اتفاقية بودابست المتعلقة بالجريمة الإلكترونية وغالبية التشريعات من الجرائم العمدية التي يجب أن يكون الجاني قد اقترفها وهو عالمٌ بحقيقتها الواقعية وبعناصرها القانونية، ويتخذ فيها الركن المعنوي صورة القصد الجنائي بعنصريه العلم والإرادة، العلم بمكونات الجريمة والإرادة إلى ارتكاب أفعال هذه الجريمة.

وفي جريمة الدخول غير القانوني للنظام المعلوماتي يتحقق القصد الجنائي بتعمد الجاني استخدام وسائل وأساليب مختلفة تمكنه من كسر شفرة الدخول وكلمات السر أو إحداث ثغرات في نظام الحماية الخاص بالنظام المعلوماتي بقصد الدخول إلى هذا النظام وهو يعلم بأنه غير مصرح له بالدخول إليه بداية أو أنه يدخل إلى مناطق داخل النظام المعلوماتي المصرح له بالدخول إليه لا يشملها هذا التصريح ويقوم بالاطلاع على المعلومات والأسرار التي يحتويها ذلك النظام. ويتحقق القصد الجنائي في جريمة البقاء غير القانوني بتعمد الجاني عند اكتشافه بأنه دخل إلى نظام معلوماتي أو إلى مناطق داخله غير مصرح له بالدخول إليها، البقاء داخله والتجول فيه والاطلاع على ما به من أسرار وبرامج.

و القصد الجنائي المطلوب لجريمة الدخول غير القانوني إلى النظام المعلوماتي قد يكون عاما أو خاصا، وهو ما يتضح من موقف التشريعات المختلفة وبيان

ذلك كالآتي:

أولا: القصد العام في جريمتي الدخول غير القانوني والبقاء غير القانوني في النظام المعلوماتي:

يراد بالقصد الجنائي العام انصراف إرادة الجاني إلى ارتكاب الجريمة مع توافر العلم بأركانها التي يتطلبها القانون و ينحصر في حدود تحقيق الهدف من الجريمة ، ويكتفي القانون بربط القصد الجنائي بالغرض الذي يسعى الجاني إلى تحقيقه بغض النظر عن الباعث الذي دفعه، فالقصد العام هو الأصل العام الكافي لقيام صورة الجريمة في الجرائم العمدية.

وبالنسبة لجريمة الدخول غير القانوني للنظام المعلوماتي فإن القصد العام يتطلب أن يكون الجاني على علم بأن دخوله إلى النظام معلوماتي كان دخولاً غير مشروع لا يستند على حق قانوني أو تصريح من مسئول النظام يخوله الدخول إلى هذا النظام أو الاطلاع على ما يحويه من معلومات أو بيانات أو برامج.

كما يقتضي القصد الجنائي إرادة الجاني حين يأتي فعله النتيجة الإجرامية التي سوف تترتب على فعله، وهذه النتيجة هي للدخول غير المصرح به إلى النظام.ومن أمثلة التشريعات التي أخذت بالقصد العام قوانين كل من فرنسا، وسلطنة عمان، والإمارات، والجزائر.ويشترط أيضاً في القصد الجنائي أن يتعاصر مع النشاط الإجرامي في جريمة الدخول غير المشروع فإذا لم يتحقق وقت الدخول ولكنه تحقق فيما بعد فإن الجريمة تكون هي البقاء غير المشروع.

ثانيا: القصد الخاص في جريمة الدخول غير المشروع:

القصد الخاص هو ذاته القصد العام من حيث أركانه إلا أن المشرع يتطلب في الجريمة حصول نتيجة إجرامية معينة، أو وقوعها بباعث خاص أو كانت الجريمة تستلزم ذلك بحسب طبيعتها ولو لم يتطلبه المشرع صراحة في نص التجريم. وبالنسبة لجريمة الدخول غير القانوني إلى النظام المعلوماتي فقد تتطلب

بعض التشريعات توافر قصدٍ خاصٍ إلى جانب القصد العام، وقد ترتب بعضها على توافر القصد الخاص تشديدا في العقوبة، ففي استراليا نص خاص بتشديد العقوبة متى ارتكب فعل الدخول غير المشروع بنية الأضرار بالغير[1]

وفي البرتغال يتطلب المشرع القصد الخاص للعقاب على جريمة الدخول غير المصرح به حيث أن قانون الجرائم المعلوماتية لسنة 1991 يعاقب (كل من يقوم على نحو غير مصرح به بالدخول إلى أنظمة أو شبكات المعلومات بنية الحصول له أو للغير على ربح أو فائدة) وتشدد العقوبة كلما كانت الفائدة أو الربح مرتفعين.[2]

وبالاتجاه ذاته أخذ نظـام مكافحة جرائم المعلوماتية السعودي لسنة 2007 حيث تطلب قصداً خاصاً لتجريم الدخول غير المشروع وذلك في المواد 3-5-7 كأن يكون الدخول غير المشروع لتهديد شخص أو ابتزازه لحمله على القيام بفعل أو الامتناع عنه, أو الدخول غير المشروع إلى موقع إلكتروني، لتغيير تصاميم هذا الموقع، أو إتلافه، أو تعديله، أو شغل عنوانه، بالإضافة إلى الدخول غير المشروع لإلغاء بيانات خاصة، أو حذفها، أو تدميرها، أو تسريبها، أو تغييرها، أو إعادة نشرها.

(1) د. أيمن عبدالله فكري – مرجع سابق – صـ274

(2) د.نائلة عادل محمد فريد قورة – مرجع سابق صـ384

الفرع الرابع

موقف المشـرع البحريني من جريمة الدخول غير القانوني

جريمة الـدخول غـير القـانوني للنظـام المعلومـاتي، هـي مـن الجـرائم الحديثـة نسـبياً، وبمراجعة قانون العقوبات البحريني والنصوص العقابية الآخرى الـواردة في قـوانين أخـرى مثل قانون الاتصالات أو قانون المعاملات الإلكترونية وغيرهما،تبـين لنـا عـدم وجـود نـص خاص يجرم أفعال الدخول غير القانوني أو البقاء غير القانوني داخل النظام المعلوماتي عـلى الرغم من خطورة تلك الأفعال على النحو السـالف بيانـه، بالإضـافة إلى أنـه في تقـديري لا يمكـن تطبيـق النصـوص العقابيـة التقليديـة وخاصـة المـادة 361 مـن قـانون العقوبـات البحريني والتي تجرم الدخول إلى مكانٍ مسكون أو معدً للسكن أو محلٍ معدً لحفظ المال أو عقار دون رضاء صاحب الشأن وفي غير الأحوال المنصـوص عليهـا قانونـاً، وتبريرذلـك أن تلك المادة نصت على سبيل الحصر الأماكن المجرم الدخول إليها، وبالتـالي لا يمكـن إدخـال أفعال الدخول أو البقاء غير القانوني داخل النظام المعلوماتي تحت هذا النص العقابي، ذلك أنه وفقاً لمبدأ الشـرعية الجنائية لا يجوز اعتبار سلوك ما جريمة مـا لم يوجـد نـص قـانوني يجرمه ويقرر لمرتكبه عقاباً محـدداً، كـما أنـه يحظـر وفقـاً لهـذا المبـدأ القيـاس للتجـريم والعقاب.

أما بالنسبة لموقف القضاء البحريني فسنستظهره في ضوء الحكمين الأتيين:

1-تخلص وقائع الدعوى في أنه في عام 2010 تلقت إدارة مكافحة الجرائم الاقتصـادية بالإدارة العامة للمباحث والأدلة الجنائية بلاغا من فتاة صغيرة جـاءت مـع والـدها لتبلـغ بأنها تعرضت لسـرقة إيميلها الخاص بواسـطة شـاب لا تعرفـه، وأنـه حـاول التقـاط صـور خاصة لها بكاميرا الكمبيوتر ولم يفلح، ولكنه نجح في الاستيلاء عـلى إيميـل لهـا بـه صـورها هي وصديقاتها، وأضافت الفتاة مقدمة البلاغ إنها فوجئت أثنـاء جلوسـها عـلى الإنترنـت،

باتصال على الماسنجر من صديقة تعرفها جيدا، فتجاوبت معها وبدأت المحادثة عادية، ولكنها بعد دقائق وجدت هذه الصديقة تخبرها بأنها مصابة بحساسية في صدرها، بسبب حمالة الصدر (السوتيان) وطلبت منها فتح الكاميرا لتريها حمالتها، وعندما ترددت أخبرتها أنهما بنتين ولا داعي للخجل، ولكنها ازدادت ريبة لأن هذه ليست طريقة صديقتها في المحادثة، فرفضت ، وطلبت منها هي أن تفتح الكاميرا لتريها صورة الحساسية، ولكن الصديقة رفضت بحجة أن هناك خللاً في الكاميرا بجهازها، واقترحت أن تتبادل معها كلمة المرور password، فأعطته كلمة المرور الخاصة بإيميل آخر، نسيت أن به صورا تخصها هي وصديقتها، واكتشفت بعد ذلك سرقة هذا الإيميل والصور، وأن التي تتحدث معها ليست صديقتها التي تعرفها، وإنما شخص سرق أيضا إيميلها وعاد ليبتزها بنشر الصور التي سرقها على الإنترنت، إذا لم تقبل بممارسة الجنس معه.وبعد أن كشفت عن صدرها اكتشفت الخدعة وكشف المتهم عن شخصيته وأنه سرق إيميلها الشخصي، وهددها بأنه سيوزع صورها إذا لم تذعن له وتقيم معه علاقة جنسية.

وقد ذكر مدير إدارة مكافحة الجرائم الاقتصادية بالإدارة العامة للمباحث والأدلة الجنائية، أنه بعد أن تم التوصل إلى عنوان الجهاز الذي استخدمه الجاني في إرسال رسائل التهديد إلى الضحية ، والقيام بتفتيش الجهاز بواسطة أحد البرامج التي تستخدمها إدارة مكافحة الجرائم الاقتصادية، والتي تكشف عن الاتصالات والرسائل التي أجراها منذ عدة سنوات، حتى لو كان قد قام بمحوها، أو حتى لو كان قد قام بإعداد عمل " فورمات" للجهاز، وتوالت المفاجآت، تبين أن الجاني أجرى محادثات مع أكثر من أربعة آلاف فتاة قام بسرقة إيميلاتهن الشخصية، وأنه سرق آلاف الصور من أولئك الفتيات وهن على الشواطئ أو في برك السباحة غير الأفلام القصيرة التي التقطها لهن بكاميرا الكمبيوتر.وتبين أنه أعاد تشغيل كافة الإيميلات التي سرقها من صاحباتها بكلمة مرورpassword واحدة، وأنه كان يتسلل إلى كافة أسماء الصديقات الواردة في قائمة الاتصالات، ومنتحلا صفة صاحبة الإيميل

الأول الذي يسرقه[1].

وقد قضت المحكمة الصغرى الجنائية بحبس المتهم سنتين حيث وجهت للمتهم تهمتين الأولى: تهديد المجني عليها بارتكاب الجريمة المعاقب عليها في المادة 355 من قانون العقوبات، وجاء التهديد مصحوبا بطلب المتهم من المجني عليها ممارسة الجنس معه، عن طريق تهديدها. والثانية،التسبب عمدا في إزعاج المجني عليها بإساءة استخدام الأجهزة السلكية واللاسلكية. وبتاريخ 15 إبريل أيدت المحكمة الكبرى الجنائية الثالثة الحكم السابق الصادر بحق المتهم[(2)].

وتعليقاً على الحكم المتقدم، فإن المحكوم عليه وفقاً للتشريعات الخاصة بمكافحة الجرائم المعلوماتية قد ارتكب جريمة الدخول العمدي بدون تصريح إلى النظام معلوماتي بقصد الاطلاع والحصول على المعلومات المخزنة به، عن طريق انتحال شخصية الغير حيث قام بخداع ضحاياه من الفتيات بأنه إحدى صديقاتهن بهدف الحصول على الأرقام السرية الخاصة بالبريد الإلكتروني الخاص بهن، حيث تمكن بهذه الوسيلة من الدخول إلى موقع البريد الإلكتروني الخاص بهن والإطلاع على معلوماتهن الخاصة وهي عبارة صورهن على الشواطئ أو في برك السباحة وغيرها. وحيث أنه لا توجد نصوصٌ أو تشريعات خاصة بالجرائم المعلوماتية بما فيها جريمة الدخول غير القانوني لنظام المعلومات في مملكة البحرين، فنلاحظ أن المحكمة لجأت إلى النصوص القانونية التقليدية وتكييفها الواقعة على أنها جريمة إزعاج المجني عليها بإساءة استخدام الأجهزة السلكية واللاسلكية المنصوص عليها في المادة (290) من قانون العقوبات البحريني والتي تنص على أنه (يعاقب بالحبس مدة لا تزيد على ستة أشهر أو بالغرامة التي لا تجاوز خمسين دينارا من تسبب عمدا في إزعاج غيره

---

(1) مجلة الأمن العام – البحرين http://www.policemc.gov.bh

(2) جريدة أخبار الخليج البحرينية – العدد رقم (12441) – الأحد 23 جمادى الأولى 1433هـ- 15 أبريل 2012 – صـ 11

بإساءة استعمال أجهزة المواصلات السلكية أو اللاسلكية.) وفي تقديري أنه لم يكن أمام المحكمة سوى تطبيق هذا النص لما يتسم به من عمومية وعدم حصره لحالات الإزعاج، والتي قد تشمل الواقعة محل الحكم باعتبار أنها انطوت على نوع من الإزعاج للضحية، وحتى لا يفلت الجاني من العقاب. وبهذه المناسبة نؤكد على ضرورة إسراع المشرع البحريني إلى إصدار تشريع خاص بجرائم المعلوماتي يكفل التصدي لهذا النوع من الجرائم، حيث أن مثل هذه الواقعة في حقيقته يتخطى مجرد إزعاج الغير، ليصل إلى انتهاك خصوصية والاعتداء على حرماتهم.

2- تتلخص وقائع هذه الدعوى حسب ما جاء بحكم محكمة التمييز البحرينية الصادر في الدعوى رقم (119/ج/2011)[1] بجلسة 30/5/ 2011 في قيام المتهم الثاني بعد أن تمكن من الحصول من خلال أحد مواقع الإنترنت على بعض أرقام البطاقات الائتمانية لأخرين ومن بينها رقم البطاقة الخاصة بالمجني عليه (ع . م) ثم تمكن من خلال محادثات (الشات) من التواصل مع المتهم الأول معتقداً أنه فتاة حيث ظلا يتبادلان الكلام العاطفي وفي إحدى مرات الاتصال عرضت عليه تلك الفتاة المزعومة (المتهم الأول) أن تعرض صوراً لأجزاء من جسدها عليه على أن يزودها بأرقام ائتمانية لاستخدامها في شحن الهواتف النقالة فأمده المتهم الثاني بأرقام البطاقات الائتمانية سالفة الذكر والتي سبق له الحصول عليها فقام المتهم الأول باستعمالها في شحن هواتف نقالة خاصة به وبأشخاص آخرين وذلك من خلال الاتصال الإلكتروني بشركة الاتصالات فتمت عملية شحن تلك الهواتف بمبالغ مختلفة ثم خصمها من حسابات أصحاب البطاقات الائتمانية سالفة الذكر دون علمهم فقام المتهم الأول باختلاس تلك المبالغ من مالكيها دون علمهم وتمت الجريمة بناء على مساعدة المتهم الثاني له على النحو المار ذكره. وكانت النيابة العامة قد اتهمت المتهمين بأنهما في غضون النصف الأول من العام 2009 بمملكة البحرين

---

(1) حكم غير منشور.

أولا: - استعملا توقيعات إلكترونية لآخرين هي الأرقام السرية لبطاقات الائتمان الخاصة بالغير، وكانت لغرض احتيالي على النحو المبين بالأوراق. ثانياً: توصلا إلى الاستيلاء على المبالغ النقدية المبينة بالأوراق والمملوكة لآخرين وكان ذلك بالاستعانة بطريقة احتيالية بأن استعملا الأرقام السرية الخاصة ببطاقاتهم الائتمانية وتمكنا بذلك من الاستيلاء على المبالغ المملوكة لهم وطلبت عقابهم بالمادة 1/391 من قانون العقوبات والخاصة بجريمة الاحتيال[1] ، وبالمادتين 1 بند (10)،1/24 بند (ج)[2] من المرسوم بقانون رقم 28 لسنة 2002 بشأن المعاملات الإلكترونية. وتم معاقبتهما على أساس هذه التهم.

وتعليقاً على الحكم السابق، نلاحظ أنه على الرغم مما ورد في الحكم من قيام المتهم الثاني من الحصول على أرقام البطاقات الائتمانية الخاصة بالمجني عليه وآخرين من خلال أحد مواقع الإنترنت، وعلى الرغم من ذلك لم تتضمن التهم المنسوبة إلى المتهم السالف بيانها، إشارة إلى دخول المتهم إلى هذا الموقع للحصول على أرقام بطاقات ائتمانية. ويستفاد من ذلك عدم وجود نص يجرم الدخول غير القانوني إلى النظام المعلوماتي والذي يشمل الدخول إلى المواقع الإلكترونية والحصول على المعلومات والبيانات المخزنة عليه، وإلا كانت النيابة العامة أسندت إليه هذه التهمة أو تصدت المحكمة لها. وهو ما يعكس وجود فراغ تشريعي يتعين الإسراع في معالجته.

---

(1) تنص المادة 1/391 من قانون العقوبات البحريني على أنه (يعاقب بالحبس من توصل إلى الاستيلاء على مال منقول أو سند أو إلى توقيع هذا السند أو إلى إلغائه أو إتلافه أو تعديله وذلك بالاستعانة بطريقة احتيالية ، أو باتخاذ اسم كاذب أو صفة غير صحيحة أو بالتصرف في عقار أو منقول غير مملوك له وليس له حق التصرف فيه...)

(2) تنص المادة (1) بند (10) من المرسوم بقانون رقم 28 لسنة 2002 بشأن المعاملات الإلكترونية على أنه (في تطبيق أحكام هذا القانون تكون للكلمات والعبارات التالية, المعاني المبينة قرين كل منها ما لم يقتض سياق النص خلاف ذلك: - التوقيع الإلكتروني: معلومات في شكل إلكتروني تكون موجودة في سجل إلكتروني أو مثبته أو مقترنة به منطقياً, ويمكن للموقع استعمالها لإثبات هويته.)

وتنص المادة 1/24 بند (ج) من ذات القانون على أنه (1 - مع عدم الإخلال بأية عقوبة أشد ينص عليها أي قانون آخر, يعاقب بالسجن مدة لا تزيد على عشر سنوات, وبغرامة لا تجاوز مائة ألف دينار أو بإحدى هاتين العقوبتين كل من ارتكب عمداً فعلاً من الأفعال الآتية: ج إنشاء أو نشر أو تحريف أو استعمال شهادة, أو توقيع إلكتروني لغرض احتيالي أو لأي غرض غير مشروع.)

المطلب الثاني

جريمة الاعتراض غير القانوني

تمثل المعلومات في الوقت الحاضر أداة مهمة لصانعي ومتخذي القرار، لذا أضحت الحاجة ملحة لتبادل وتداول تلك المعلومات بسرعة ودقة، وقد ساعد تطور وسائل تكنولوجيا المعلومات والاتصالات وظهور الشبكات الإلكترونية والأقمار الصناعية وغيرها من وسائل الاتصالات ونقل البيانات في تلبية تلك الحاجة.وأمام المخاطر والتهديدات المتزايدة المحيطة بعملية نقل البيانات والمعلومات عبر وسائل الاتصالات الحديثة، نتيجة لإساءة استخدام تلك الوسائل المتقدمة من قبل بعض الأشخاص لتحقيق أغراضهم الإجرامية، أضحت الحاجة ملحة إلى ضمان أمن وسلامة تلك المعلومات وضمان سريتها.

وفي تقديري تعد جريمة الاعتراض غير القانوني للمعلومات أو التقاط المعلومات من قبيل أعمال التجسس المعلوماتي والذي ينشط بشكل كبير في المجالات السياسية والعسكرية والتجارية بين الكثير من الدول والشركات التجارية كما سبق الإشارة إليه في مواضع أخرى من هذا البحث[1]. وسنبين من خلال هذا المطلب بشكل مفصل جريمة الاعتراض غير القانوني من حيث بيان مفهوم فعل الاعتراض، وأركان الجريمة ووسائل ارتكابها، ولكننا سنمهد لذلك كله بإعطاء صورة عامة عن عملية نقل البيانات من الناحية الفنية بما يساعدنا على فهم هذه الجريمة واستيعابها.

---

(1) راجع صـ 18 – 20 من هذا البحث.

الفرع الأول

كيفية نقل البيانات والمعلومات الإلكترونية

من ضروريات البحث في الجرائم المعلوماتية بما فيها جريمة الاعتراض غير القانوني نظراً لطابعها الفني والتقني فضلا عن حداثتها النسبية، أن يلم كلٌّ من الباحث والقارئ ببعض الجوانب الفنية المرتبطة بتلك الجريمة، والتي تساعده على استيعابها وفهمها بشكل أكثر دقة. ومن هذا المنطلق سنستعرض في هذا الجزء من البحث كيفية نقل البيانات والمعلومات عبر وسائل الاتصالات المختلفة، وهو ما سيمهد لنا استيعاب أساليب مرتكبي هذه الجرائم، والتي سنتناولها لاحقا.

تتعدد وتتنوع الوسائل والقنوات التي تستخدم في نقل المعلومات والبيانات فمنها السلكي واللاسلكي، ومنها الأرضي ومنها ما هو عبر الفضاء مثل الأقمار الصناعية، وتوضيح ذلك على النحو الأتي:

1- خطوط التليفون:

تعد الخطوط التليفونية من أهم الابتكارات التي شهدتها الإنسانية، ويعود الفضل فيه للمخترع إسكندر جراهام بيل الذي اخترع التليفون عام 1876م.

كما تعد وسيلة التليفون من أفضل وسائل الاتصالات في توصيل المعلومات الصوتية أو المسموعة، حيث يتم استخدام شبكة خطوط التليفون في نقل الأصوات والإشارات التليفزيونية والصور والبيانات الرقمية الصادرة من أجهزة الكمبيوتر، والمعلومات المقروءة آليا بواسطة جهاز الكمبيوتر.وهناك عدة وسائل اتصالات مرتبطة بالخطوط التليفونية مثل:

أ) الفاكسميل (Facsimile)، والذي يستخدم لنقل المعلومات المصورة بواسطة التليفون.

ب) التليتايب (Teletype) والذي يقوم بطبع البرقيات من بعد حيث

تطبع العلامات المرسلة والمستقبلة بدلا من سماعها.

ج) الوصول المباشر (Online) وذلك باستخدام الكمبيوتر مع خطوط التليفونات المرتبطة بالنهايات الطرفية وأجهزة الوصول (Modems)، حيث يعطى جهاز الكمبيوتر رقما تليفونيا خاصا به كما الأفراد العاديين، وبالتالي فإنه يمكن الاتصال به، ويتم التأكد من بدء الاتصال المباشر مع الكمبيوتر وبأنه أصبح في حالة استقبال وإرسال للمعلومات، عند سماع أو تلقي أي إشارة صوتية أو مرئية على شاشة النهاية الطرفية.

د) اللمس النغمي التليفوني (Touch Tone Telephone) تمكن هذه الوسيلة المستخدم من إرسال معلوماته أو بياناته مباشرة إلى الكمبيوتر عن طريق نبضات صوتية مختلفة تمثل كل رقم متواجدة على مفاتيح لمس خاصة بذلك، وبهذا يمكن توصيل البيانات الرقمية مباشرة إلى جهاز الكمبيوتر والذي يقوم بدوره بمعالجتها[1].

2- الكابلات (Cables):

على الرغم من فاعلية خطوط الاتصال التليفونية في نقل المحادثات الصوتية والبيانات الرقمية، إلا أن نمو عملية نقل وتبادل المعلومات والبيانات رافقه رغبة في توفير وسيلة آخرى أو قنوات اتصال آخرى تكون قادرة على نقل كميات كبيرة من المعلومات والبيانات المقروءة آليا والمتداولة بين أجهزة الكمبيوتر بصورة أسرع وأكثر كفاءة وفاعلية من خطوط الاتصال التليفوني التي باتت تستغرق وقتا طويلا في نقل البيانات والمعلومات بين أجهزة الكمبيوتر المرسلة والمستقبلة نظرا لمحدودية طاقتها في نقل كميات كبيرة من المعلومات والبيانات، لذا تم اللجوء إلى استخدام الكابلات كوسيلة من وسائل الاتصالات لنقل البيانات. وتنقسم الكابلات إلى عدة أنواع[2] أهمها ما يأتي:

---

(1) د. محمد محمد الهادي - تكنولوجيا المعلومات وتطبيقاتها - دار الشروق - القاهرة - الطبعة الأولى 1989م صـ 156 - 158

(2) حسن طاهر داود- مرجع سابق - صـ 54 - 60

أ- الخطوط المجدولة (أو السلك الملتوي) Twisted-Pair lines:

هو الأكثر شعبية في الوقت الحاضر وتشبه هذه الخطوط سلك الهاتف وهو مكون من (8) أسلاك داخلية وليس (2) كما في حالة الهاتف، وسمي (بالملتوي) بذلك لأن كل سلكين من الثمانية يكونان ملفوفان وبهذا يكون هناك أربعة أزواج من تلك الأسلاك [1]. ويصلح هذا النوع من قنوات الاتصال لنقل بيانات بسرعة في حدود (1 Mbps)[2] عبر مسافات قصيرة حوالي (100 متر) أو بنقل سرعات أقل لمسافات أطول، ويمكن زيادة سرعة النقل وزيادة مسافات النقل عن طريق استخدام دوائر استقبال متطورة.

ب- الكابلات المحورية Coaxial Cable:

هو نوع من أنواع الكابلات النحاسية ويشتمل على حزمة من الأسلاك المعزولة عن بعضها البعض وتحميها أغلفة واقية،يستخدم هذا النوع لنقل كميات ضخمة من البيانات[3] ويستخدم هذا النوع من الكابلات للتطبيقات التي تحتاج إلى سرعات نقل بيانات أعلى من (1 Mbps)، حيث يمكن استخدامه للترددات التي تصل إلى (10 Mbps) وعبر مسافات تصل إلى عدة مئات المترات.

ج- كابلات الألياف الضوئية:

كابلات الألياف الضوئية هي عبارة عن أسلاك مصنوعة من الزجاج النقي رقيقة جدا - بمثل رقة شعر الإنسان - تستخدم لنقل الإشارات الرقمية إلى

---

(1)http://ar.wikipedia.org

(2) **Mbps** : هو اختصار لـ (Megabits Per Second) ميغابت في الثانية .وهو معدل يشير إلى سرعة نقل البيانات مقاسا في ميغابت (1 mbps (megabit per second) = 1,000,000 bits per second)، (**البت** -bit)يتم في الحواسيب تخزين المعلومات ومعالجتها على شكل بتات (bits) وبذلك يكون نظريا البت أصغر وحدة حاملة أو ناقلة لمعلومة أو لمعنى معين.

وفي الحواسيب والمعالجات الرقمية، البت هو عبارة عن نبضة كهربائية إما موجبة أو سالبة ،ويرمز لها بأحد الرقمين الثنائيين. إما 1 أو 0. المرجع

- http://www.wisegeek.com/what-is-mbps.htm.

(3) د. محمد محمد الهادي – مرجع سابق- صـ164

مسافات طويلة. حيث تقوم بنقل البيانات في صورة شعاع متردد من الضوء في وسط من الألياف الزجاجية، ولا توجد أسلاك نحاسية أو إشارات كهربائية. لقد أحدثت الألياف الضوئية ثورة في عالم الاتصالات وتفوقت على أسلاك التوصيل العادية في القدرة على حمل المعلومات ويعود ذلك إلى أن الألياف الضوئية مكونة من أسلاك رقيقة جدا ارفع من الأسلاك العادية، لذا فأنه يمكن وضع عدد كبير منها داخل الحزمة الواحدة مما يزيد عدد خطوط الهاتف أو عدد قنوات البث التلفزيوني في حبل واحد. بالإضافة إلى عدم إمكانية تداخل الإشارات المرسلة من خلال الألياف المتجاورة في الحبل الواحد مما يضمن وضوح الإشارة المرسلة سواء أكانت محادثة تلفونية أو بث تلفزيوني[1]. كما أنها لا تتعرض للتداخلات الكهرومغناطيسية مما يجعل الإشارة تنتقل بسرية تامة مما له أهمية خاصة في الأغراض العسكرية[2]. كما يمتاز هذا النوع من الكابلات بسرعة نقل البيانات والمعلومات بسرعات تصل باستخدام وسائل الاستقبال المناسبة إلى (500 Mbps)[3].

3- الأقمار الصناعية:

لا يقتصر نقل البيانات والمعلومات على الوسائل أو الوسائط المادية السابقة، حيث يمكن نقلها باستخدام وسائل أكثر تطور مثل موجات الراديو (الموجات الكهرومغناطيسية) من خلال الفضاء الخارجي عبر الأقمار الصناعية.

وتعد الأقمار الصناعية من وسائل الاتصالات عن بعد الحديثة التي تستخدم في نقل البيانات والمعلومات، ومنذ عام 1970، أصبح الاعتماد كبيراً ومتزايداً على الأقمار الصناعية، في مجال الاتصالات، ويلاحظ ذلك من أعداد الأقمار الصناعية الكثيرة التي بات المدار الفضائي مزدحماً بها[4]. وتمتاز الأقمار الصناعية

---

(1)http://ar.wikipedia.org ، http://ar.hicow.com

(2) http://www.aviadef.com/article.aspx?magid=43&artid=11&PageIndex=3

(3) حسن طاهر داود- مرجع سابق – صـ 57

(4) يتم إطلاق القمر الصناعي بواسطة صاروخ ضخم ليضعه في المدار الجوي فوق الارض، على ارتفاع 23 ألف ميل تقريبا. وبالنسبة لحجم القمر الصناعي فيبلغ أرتفاعه حوالي (10) أقدام وعرضه حوالي (8) اقدام، ويشتمل القمر الصناعي على عدة أجهزة لاستقبال الرسائل من المحطات الارضية وتقوم ببثها إلى الوجهة المحددة. والقمر الصناعي مزود بمجموعة من البطاريات الشمسية التي تستمد طاقتها من الشمس=

بسعتها الكبيرة والتي تصل إلى (500 Mbps) ويستطيع توفير المئات من خطوط نقل البيانات بسرعة عالية. وتقسم سعة القناة القمرية إلى قنوات فرعية يخصص كل منها لخط نقل بيانات معين [1] . وتتميز الأقمار الصناعية بالإضافة إلى سعة الاستيعاب بسرعة الإنشاء، وكفاءة الإرسال والاستقبال على مسافات تقاس بآلاف الأميال، إضافة إلى التكلفة المنخفضة.وتتلخص فكرة الاتصال عبر القمر الصناعي، في أن المحطة الأرضية تُرسل إشاراتها المحمّلة بالمحادثات الهاتفية والبرامج الإذاعية والتليفزيونية والصور والخرائط والبيانات الرقمية إلى القمر الذي يلتقطها، ويكبّرها، ثم يعيد إرسالها إلى محطات الاستقبال الأرضية. وبذلك، فإن قمر الاتصالات، من حيث فكرة عمله، يَسْتخدم الموجات متناهية القصر "الميكروويفMicrowaves" ، التي يمكنها أن تحمل كمّاً هائلاً من المعلومات، ولكنها تسري في خطوط مستقيمة. ولذا، فإن التغلب على كروية الأرض، يجعل من المحتوم وضع محطات إعادة الإرسال على مسافات لا تزيد على 50 كم من بعضها بعضاً .وهو أمر يمكن تنفيذه ـ إلى حدٍّ ما ـ على الأرض، بينما يتعذر تحقيقه في المحيطات والبحار.[2]

4- أشعة الميكروويف (Microwave):

تستخدم خطوط الاتصال باستخدام أشعة الميكروويف كوسيلة أو قناة اتصال في نقل البيانات والمعلومات عن بعد عن طريق الموجات متناهية الصغر والعالية التردد للطيف الإذاعي الذي ينقل البيانات والرسائل الصوتية، وتتميز هذه الوسيلة بأنها عملية لنقل البيانات عن الكابلات أو الوسائط المادية واقل تكلفة، وخاصة بالنسبة للمناطق التي يصعب مد كابلات فيها مثل البحار أو الصحراء، أو لارتفاع تكلفة القيام بذلك. ويتطلب نقل البيانات بواسطة أشعة الميكروويف وجود خط رؤية مفتوح دون عوائق بين طبق الإرسال وطبق

=مباشرة والتي يتم تحويلها إلى طاقة كهربائية لتشغيل القمر،ويستمر دوران القمر الصناعي في مداره في الفضاء لستت اعوام تقريبا قبل استبداله بأخر. - راجع - د. محمد محمد الهادي - مرجع سابق- صـ 166-167

(1) حسن طاهر داود- مرجع سابق- صـ 61

(2) المرجع نفسه- صـ 66

الاستقبال.[1]

-5 **موجات الراديو (Radio waves) :**

موجات الراديو هي جزء من طيف الموجات الكهرومغناطيسية وتنـتج تلـك الموجـات في الطبيعة عن طريق البرق أو الأجسام الفلكية، وتستطيع الأجهزة التي تعمل بموجات الراديو نقل كمية كبيرة من المعلومات، وبسـرعة عالية، بـين جهـازين إلكترونيـين، لـذا تسـتخدم في مجال البث الإذاعي الثابت والمتحرك، مثل الراديو والتلفزة واتصـالات الخلـوي والملاحـة،كما ترسل شـركات الهاتف والبرق الرسائل بوساطة الراديـو حيـث تسـتخدم موجـات الراديـو في نقل صور الفاكسميلي، حيث تحول الصور إلى إشارات إلكترونية ترسل بموجات الراديو ، كما يستخدم الجواسيس أجهزة تعمل بموجات الراديو للتنصت على المحادثات بغـرض الحصـول على المعلومات السـرية ويستخدم أيضاً في شبكات الكمبيـوتر[2]،حيـث يمكـن توصيـل عـدد كبير من أجهزة الحاسبات الآلية المنتشـرة في مناطق مختلفة في الدولة بهدف جمع البيانات مثال توصيل أجهزة الحاسبات الآلية المستخدمة في منافذ الجوازات البرية والبحرية والجوية بالدولة حيث يتم تجميع البيانات المدخلة مـن هـذه الأجهـزة وتخزينهـا في جهـاز مركـزي، ويتم استخدام موجات الراديو لتشكل شبكة لاسلكية بين نقطة محـددة وعـدد مـن أجهـزة الحاسب الآلي الموزعة ويتم ذلك عن طريق جهاز إرسال يسـمى (القاعـدة – Base station) في النقطة المركزية الثابتة[3].

---

(1) المرجع نفسه – صـ 64

(2)http://ar.wikipedia.org ، http://www.marefa.org

(3) حسن طاهر داود- مرجع سابق- صـ 64

الفرع الثاني

الركن المادي لجريمة الاعتراض غير القانوني

أولا: مفهوم الاعتراض غير القانوني:

عرفت المادة الثالثة من اتفاقية بودابست المتعلقة بالجريمة الإلكترونية الاعتراض غير القانوني بأنه (... واقعة الاعتراض العمدي وبدون حق، من خلال وسائل فنية للإرسال غير العلني، لبيانات الحاسب، في مكان الوصول، في المنشأ، أو في داخل النظام المعلوماتي، بما في ذلك الانبعاثات الكهرومغناطيسية من جهاز حاسب يحمل هذه البيانات...)

ولقد بينت المذكرة التفسيرية للاتفاقية المذكورة بأن الهدف من هذه المادة هو حماية الحق في حرية الاتصالات واحترام نقل البيانات،حيث أن هذه الجريمة تشكل انتهاكاً للحق في احترام الاتصالات مثل التنصت أو تسجيل المحادثات التليفونية بين الأشخاص، ناهيك عما تشكله هذه الجريمة أيضا من انتهاك لحق احترام المراسلات الذي تكفله المادة الثامنة من الاتفاقية الأوروبية لحقوق الإنسان[1]، وأن هذه المادة على هذا النحو تطبق هذا المبدأ على كل صور النقل الإلكتروني للبيانات والمعلومات، سواء عن طريق التليفون أو الفاكس أو البريد الإلكتروني، أو نقل الملفات.[2]

---

(1) تنص المادة (8) من الاتفاقية الأوروبية لحقوق الانسان المبرمة في 4 نوفمبر 1950 على أن (1- لكل إنسان حق احترام حياته الخاصة، والعائلية ومسكنه ومراسلاته.2- لا يجوز للسطة العامة أن تتعرض لممارسة هذا الحق إلا وفقاً للقانون وبما تمليه الضرورة في مجتمع ديمقراطي لصالح الأمن القومي وسلامة الجمهور أو الرخاء الاقتصادي للمجتمع، أو حفظ النظام ومنع الجريمة، أو حماية الصحة العامة والاداب، أو حماية حقوق الاخرين وحرياتهم.) ، المرجع ، أ.د محمود شريف بسيوني، خالد محيي الدين - الوثائق الدولية والإقليمية المعنية بحقوق الإنسان - المجلد الثالث - دار النهضة العربية - القاهرة -ص 138

(2) د. هلالي عبداللـه احمد - مرجع سابق - ص 78 - 79.

وفي مفهوم آخر لهذا الفعل، فيقصد به الاعتراض عن طريق وسائل فنية للاتصال توجه لنظام كمبيوتر أو عدة نظم أو شبكة اتصالات.[1]

وفي ضوء ما سبق فإنه يمكننا تعريف الاعتراض غير القانوني،(بأنه أي نشاط غير مشروع يهدف إلى الاطلاع على محتوى اتصال من بيانات ومعلومات تتم داخل نظام حاسب آلي واحد، أو أكثر تربطها شبكة اتصالات باستخدام الوسائل الفنية التي تمكنه من ذلك.)

ومن خلال استطلاع التشريعات المختلفة التي تناولت جريمة الاعتراض غير القانوني للبيانات، نلاحظ أنها انقسمت إلى اتجاهين بالنسبة لاشتراط استخدام وسائل فنية في ارتكاب الجريمة، وبيان ذلك على النحو الآتي:

الاتجاه الأول: الذي لا يشترط استخدام وسائل فنية في ارتكاب جريمة الاعتراض غير القانوني:

يتضمن هذا الاتجاه ، - وهو ما نميل إليه - وجوب النص على صور الفعل المادي المكون لجريمة الاعتراض غير القانوني وهي التنصت أو الالتقاط أو الاعتراض العمدي من دون وجه حق ،لكل ما هو مرسل عن طريق الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات أيا كانت الوسيلة المستخدمة ،وهو الجانب الأهم من التجريم حيث يعطي النص قدراً كبيراً من المرونة والقابلية للتناول الوسائل الفنية المختلفة، ولتفادي أي خلاف قد ينشأ حول الوسيلة وما يعتبر منها وسيلة فنية أو تقنية وما لا يعتبر كذلك. ومن التشريعات التي تبنت هذا الاتجاه نظام مكافحة جرائم المعلوماتية السعودي لسنة 2007 حيث تنص الفقرة الأولى من مادته الثالثة على أنه (يعاقب بالسجن مدة لا تزيد على سنة

(1) حاء هذا التعريف ضمن مقررات وتوصيات المؤتمر الخامس عشر للجمعية الدولية لقانون العقوبات 4-9 تشرين اول 1994 - البرازيل / ريو دي جانيرو بشأن جرائم الكمبيوتر اذ انه من بين توصيات المؤتمر ان تتضمن قائمة الحد الادنى للأفعال المتعين تجريمها واعتبارها من قبيل جرائم الكمبيوتر. 1- الاحتيال أو الغش المرتبط بالكمبيوتر. 2- تزوير الكمبيوتر أو التزوير المعلوماتي. 3- الاضرار بالبيانات والبرامج (الاتلاف). 4- تخريب واتلاف الكمبيوتر. 5- الدخول غير المصرح به. 6- الاعتراض غير المصرح به.... للاطلاع على مقرارات وتوصيات هذا المؤتمر راجع كتاب د. عبدالفتاح مراد - مرجع سابق صـ240-243

وبغرامة لا تزيد على خمسمائة ألف ريال، أو بإحدى هاتين العقوبتين ؛ كل شخص يرتكب أياً من الجرائم المعلوماتية الآتية:1- التنصت على ما هو مرسل عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي - دون مسوغ نظامي صحيح - أو التقاطه أو اعتراضه....). وبهذا أخذ أيضاً قانون مكافحة جرائم تقنية المعلومات الإماراتي لسنة 2006 حيث تنص مادته الثامنة على أن (كل من تنصت أو التقط أو اعترض عمداً، من دون وجه حق، ما هو مرسل عن طريق الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات، يعاقب بالحبس وبالغرامة أو بإحدى هاتين العقوبتين)

الاتجاه الثاني: الذي يشترط استخدام وسائل فنية في ارتكاب جريمة الاعتراض غير القانوني

فقد تبنت اتفاقية بودابست المتعلقة بالجريمة الإلكترونية هذا الشرط وذلك بموجب المادة الثالثة منها حيث نصت على أنه (يجب على كل طرف أن يتبنى الإجراءات التشريعية أو أية إجراءات آخرى يرى أنها ضرورية من أجل اعتبارها جريمة جنائية،.... واقعة الاعتراض العمدي وبدون حق، من خلال وسائل فنية للإرسال غير العلني، لبيانات الحاسب، في مكان الوصول، في المنشأ، أو في داخل النظام المعلوماتي، بما في ذلك الانبعاثات الكهرومغناطيسية من جهاز حاسب يحمل هذه البيانات...). وعلة هذا الشرط وفقا لما ورد بالمذكرة التفسيرية لهذه الاتفاقية، أنه يعد مقيداً لتجنب العقاب المبالغ فيه [1]. وقد أخذ بهذا الاتجاه القانون البرتغالي الخاص بجرائم المعلوماتية الصادر في عام 1991، حيث جرم اعتراض عمليات الاتصال التي تقوم على نقل المعلومات داخل أنظمة الحاسبات الآلية أو شبكات المعلومات باستخدام وسائل تقنية[2])

وباستقراء نصوص بعض التشريعات العربية الخاصة بجرائم المعلوماتية، نلاحظ أن قانون مكافحة جرائم تقنية المعلومات العماني لسنة 2011 قد أخذ

---

(1) د. هلالي عبداللـه احمد – مرجع سابق – صـ 80.

(2) د.نائلة عادل محمد فريد قورة – مرجع سابق – صـ364 - 365

بذات الاتجاه حيث نصت المادة (8) منه على أنه (يعاقب بالسجن مدة لا تقل عن شهر ولا تزيد على سنة وبغرامة لا تقل عن خمسمائة ريال عماني ولا تزيد على ألفي ريال عماني أو بإحدى هاتين العقوبتين، كل من اعترض عمداً ودون وجه حق باستخدام وسائل تقنية المعلومات خط سير البيانات أو المعلومات الإلكترونية المرسلة عبر الشبكة المعلوماتية أو وسائل تقنية المعلومات أو قطع بثها أو استقبالها أو تنصت عليها)

وفي ضوء ما تقدم، فإنه وفقا لهذا الاتجاه يشترط في فعل الاعتراض المكون للركن المادي لجريمة الاعتراض غير القانوني أن يكون باستخدام وسائل فنية معدة للتصنت أو نقل البيانات وتسجيلها أو التحكم والحصول على المحتويات بصورة مباشرة أو بواسطة الدخول إلى النظام المعلوماتي، وكذلك يمكن أن تشمل الأجهزة الفنية المتصلة بخطوط النقل أو الاتصال مثل أجهزة تجميع وتسجيل الاتصالات اللاسلكية، وسنوضح فيما يلي وسائل اعتراض نقل البيانات والمعلومات.

ثانيا وسائل اعتراض نقل البيانات والمعلومات:

عرفت الجماعات البشرية منذ القدم عمليات التجسس والتنصت من أجل الحصول على المعلومات، وابتدعت في سبيل ذلك كافة الوسائل التي تمكنها من ذلك. وانعكس التطور الذي شهدته البشرية وظهور عصر المعلومات والاتصالات على وسائل التجسس والتنصت التي تحولت من مجرد وسائل بدائية بسيطة إلى وسائل إلكترونية أكثر دقة واحترافية تتناسب ومتطلبات العصر الحديث.

ويعد الاعتراض أو الالتقاط غير القانوني هو أحد مظاهر التجسس الإلكتروني الذي يقوم على رصد ومراقبة أجهزة الحاسب الآلي، عن طريق التسلل إليها أو محاولة اعتراض الإشارات وحزم المعلومات التي ترسل من قبل هذه الأجهزة عبر شبكات المعلومات التي تربط بين معظم الحواسيب،بهدف الحصول على تلك المعلومات والتي يحرص مالكيها على بقائها طي الكتمان. ونستعرض من خلال ما يأتي أهم الوسائل المستخدمة في عمليات اعتراض

والتقاط المعلومات والبيانات الإلكترونية:

1- مراقبة الرسائل:

يقوم المهاجم باستخدام برامج الكترونية تقوم بمراقبة حزم الرسائل لمعرفة ما بداخلها، ويتم ذلك بشكل آلي[1]. ويهدف المهاجم من قيامه بمراقبة الرسائل الحصول على معلومات مهمة يتوقع وجودها داخل الرسالة ككلمات السر[2] أو أرقام بطاقات الائتمان.

2- إعادة إرسال الرسائل :

يقوم المهاجم في هذه الحالة بالتقاط المعلومات عند مرورها ثم يقوم بتخزينها ثم يعيد إرسالها مرة آخرى فيما بعد، وقد تتم هذه العملية بشكل انتقائي أي يقوم المهاجم باختيار المعلومات التي يتم تخزينها و إعادة إرسالها بشكل انتقائي ويعتمد ذلك على قدرة المهاجم على تمييز المعلومات التي يسعى وراءها مثال(كلمات السر). وقد تتم دون تمييز حيث يقوم المهاجم في هذه الحالة بإعادة إرسال حزم الرسائل كلها دون تمييز.[3]

---

(1) ومن أهم تطبيقات نظام مراقبة الرسائل (Packet Sniffer) برنامج (كارنيفور) Carnivore وهي كلمة إنجليزية تعني آكل اللحوم إشارة إلى أن البرنامج يقوم بمضغ كافة البيانات المتدفقة عبر شبكة ما، ووفقا لوكالة المباحث الفيدرالية الأمريكية فإن كارنيفور هو نظام كومبيوتري مصمم ليسمح لوكالة المباحث الفيدرالية الأمريكية، وبالتعاون مع الشركة المزودة لخدمات إنترنت، بتطبيق أمر محكمة بجمع معلومات محددة حول رسائل البريد الإلكتروني، أو أية اتصالات إلكترونية أخرى من وإلى مستخدم معين يستهدفه تحقيق ما، ويمكن استخدام برنامج كارنيفور بطريقتين هما:

- **الأولى**: رصد المعلومات الواردة إلى والصادرة من حساب بريد إلكتروني معين، أو رصد حركة البيانات من وإلى عنوان IP معين. ويتم ذلك بعدة طرق وذلك إما من خلال رصد جميع الترويسات headers الخاصة برسائل البريد الإلكتروني (بما في ذلك عناوين البريد الإلكتروني) الصادرة من والواردة إلى حساب معين، ولكن ليس المحتويات الفعلية (أو خانة الموضوع).

- **الثانية** : رصد جميع الأجهزة المزودة (مزودات الويب، والملفات) التي يقوم المشتبه به بالنفاذ إليها، وذلك من دون رصد المحتوى الفعلي لما ينفذ المستخدم إليه. ويمكن أيضا رصد جميع المستخدمين الذين يقومون بالنفاذ إلى صفحة ويب معينة أو ملف باستخدام FTP وأخيرا، يمكن رصد جميع صفحات إنترنت، وملفات FTPالتي يقوم المستخدم بالنفاذ إليها. وتجدر الإشارة إلى أن برنامج كارنيفور لا يقوم بتغيير البيانات التي يقوم بجمعها، وإنما تقتصر مهمته على التصنت على الحزم وتسجيل نسخة منها - المرجع - http://ar.wikipedia.org

(2) حسن طاهر داود- مرجع سابق- صـ 128 ، -http://coeia.edu.sa/ar/asuurance-awarness/articles/52 network-security/467-ip-security.html

(3) المرجع - نفسه - صـ 131 - 132

3- **التقاط الإشعاعات التي تصدر عن الأجهزة:**

يقوم الجاني في هذه الصورة بالتقاط الإشعاعات التي تصدر عن الأجهزة ثم يتم تسجيلها ومن ثم حل شفرتها بواسطة أجهزة الكترونية ومثال ذلك فان آلات الطابعة المرتبطة بالحاسب الآلي تمتاز بطبيعتها السريعة ويصدر عنها إشعاعات إلكترومغناطيسية أثناء عملها، وفي هذه الحالة يقوم الجاني بربط الطابعة المستخدمة في ارتكاب الجريمة مع الطابعة الموجودة داخل المركز المعلوماتي محل الجريمة ثم يطلب منها نسخ هذه المعلومات المتداولة حرفيا[1].

4- **اختطاف جلسة الاتصال الشبكي:**

يتم انتقال البيانات بين أي طرفين متصلين فيما بينهما على الشبكة على شكل حزم تنتقل بين هذين طرفين ، وفي لحظة ما يقوم المهاجم بواسطة استخدام أسلوب اختطاف جلسة الاتصال الشبكي التجسس على هذه الحزم وخطف الاتصال،عن طريق تحديد أحد أطراف الاتصال وإيهام الطرف الآخر باستمرارية الاتصال مع الجهاز الأصلي في حين يكون الاتصال قد أصبح بين الجهاز الضحية وجهاز الهكر وبذلك يتمكن المهاجم من تنفيذ أوامر على الجهاز الضحية[2].

وتجدر الإشارة إلى أنه يمكن لجوء سلطات التحقيق إلى استخدام إحدى الوسائل السابقة بإذن من السلطة المختصة بمناسبة التحقيق في قضية ما، أو بهدف تتبع بعض المجرمين أو المشتبه فيهم، أو قد يتم هذا الاعتراض بموافقة مالكي المعلومات أو الشبكات أو النظم المعلوماتية وهم بصدد اختبار درجة أمان وسيلة نقل البيانات ومدى إمكانية اختراقها. لذا فإنه يشترط في فعل الاعتراض أن يكون غير قانوني، وهو ما سنبينه الجزئية التالية.

---

(1) د. محمد علي العريان - مرجع سابق صـ75

(2) د. حسين بن سعيد الغافري - الجاسوسية الرقمية - مقال منشور على الموقع الالكتروني: http://www.omanlegal.net

ثالثا: يشترط أن يكون فعل الاعتراض غير قانوني:

يشترط في فعل الاعتراض أن يكون بدون وجه حق غير قائم على سند من القانون، أي دون تصريح من صاحب الشأن أو في غير الحالات التي نص عليها القانون، حيث أنه من المتصور أن الشخص الذي قام باعتراض البيانات أو المعلومات التي يتم نقلها عبر الشبكات والتنصت عليها وتسجيلها، قد قام بذلك بناء على ذوي الشأن ممن لهم سلطة على البيانات والمعلومات أو الشبكة المعلوماتية أو قناة نقل البيانات، بهدف اختبار أنظمة حماية الشبكة المعلوماتية أو قناة نقل البيانات واكتشاف الثغرات الأمنية بها تمهيدا لعلاجها وتطوير أنظمة حمايتها.

كما قد يتم مراقبة نقل البيانات والمعلومات والتنصت عليها وتسجيلها بموجب تصريح من السلطة القضائية في الأحوال المقررة قانوناً وفي هذه الحالة يجب أن يتم ذلك في نطاق الإذن الموضوعي والزمني، بحيث إذا ما ارتكبه بعد انتهاء المدة المحددة في الأذن كان مرتكبا لجريمة الاعتراض غير القانوني ، مثال ذلك ؛ تنص المادة (93) من قانون الإجراءات الجنائية البحريني رقم (46) لسنة 2002 على أنه (يجوز للنيابة العامة أن تضبط لدى مكاتب البريد جميع الخطابات والرسائل والجرائد والمطبوعات والطرود ، ولدى مكاتب البرق جميع البرقيات، وأن تراقب المحادثات والمراسلات السلكية واللاسلكية أو إجراء تسجيلات لأحاديث جرت في مكان خاص متى كان لذلك فائدة في ظهور الحقيقة في جناية أو جنحة معاقب عليها بالحبس. ويشترط لاتخاذ أي من الإجراءات السابقة الحصول مقدما على إذن بذلك من قاضي المحكمة الصغرى، ويصدر القاضي هذا الإذن بعد اطلاعه على الأوراق.وفي جميع الأحوال يجب أن يكون الضبط أو المراقبة أو التسجيل بناء على أمر مسبب ولمدة لا تزيد على ثلاثين يوما قابلة للتجديد لمدة أو مدد آخرى مماثلة.)

أو قد يتم ذلك بناء على السلطة المختصة في الحالات المتعلقة بالأمن القومي للدولة مثال ما نصت عليه المادة (29) من قانون حماية المجتمع من الأعمال

الإرهابية البحريني رقم (58) لسنة 20006 من أنه (للمحامي العام أو من يقوم مقامه أن يأمر بضبط الرسائل بجميع أنواعها والمطبوعات والطرود والبرقيات، وبمراقبة الاتصالات بجميع وسائلها، وتسجيل ما يجرى في الأماكن العامة أو الخاصة، متى كان لذلك فائدة في كشف الحقيقة في الجرائم التي تنطبق عليها أحكام هذا القانون.

وفي جميع الأحوال يجب أن يكون أمر الضبط أو المراقبة أو التسجيل مسبباً ولمدة لا تجاوز ستين يوماً، ولا يجوز مد هذه المدة إلا بأمر من المحكمة الكبرى.)

الفرع الثالث

الركن المعنوي لجريمة الاعتراض غير القانوني

تعد جريمة الاعتراض غير القانوني للمعلومات والبيانات الإلكترونية من الجرائم العمدية التي يتطلب فيها القصد الجنائي بعنصريه العلم والإرادة وذلك وفقا لما ذهبت إليه مختلف التشريعات الخاصة بالجرائم المعلوماتية. فيجب أن يكون الجاني قد اقترفها وهو عالمٌ بحقيقتها الواقعية وبعناصرها القانونية.

وفي جريمة الاعتراض غير القانوني للنظام المعلوماتي يتحقق القصد الجنائي بتعمد الجاني استخدام وسائل التقاط واعتراض وتسجيل البيانات والمعلومات الإلكترونية أثناء عملية نقلها والتصنت عليها والاطلاع على محتواها دون رضاء أو تصريح من أطراف الاتصال، أو سند من القانون. فإذا تخلف لديه هذا العلم بأن كان يعتقد على خلاف الحقيقة بأنه مصرح له بحكم عمله لدى الشركة مزودة خدمة الاتصالات بالاطلاع على البيانات المنقولة أو مراقبتها على نحو فيه خطأ في تفسير حدود اختصاصاته، أو أنه دخل إلى نطاق الاتصال بالخطأ وتوقف نشاطه عند هذا الحد، حيث أنه إذا استمر في التصنت بعد علمه بأنه دخل إلى نطاق اتصال غير مرخص له الوصول إليه، فإنه في هذه اللحظة يكون قد نشأ لديه القصد الجنائي المطلوب لتحقق جريمة الاعتراض غير القانوني.

كما يجب أن تكون قد اتجهت إرادته الحرة إلى ارتكاب الأفعال المكونة للسلوك المادي لهذه الجريمة وهو التصنت أو التقاط أو تسجيل البيانات والمعلومات، فقد يأتي الفاعل هذه الأعمال تحت تأثير تهديد وإكراه من قبل آخرين لاستغلال مهارته وخبرته في مجال الاتصالات واستخدام أجهزة الحاسبات الآلية وما يتمتع به من قدرة على اختراق الشبكات ونظم المعلومات.

وقد يرتكب الفاعل هذه الأفعال نتيجة لخداع أو استغلال وهو ما قد يتصور بالنسبة لصغار السن الذين يحترفون استخدام أجهزة الحاسبات الآلية ويملكون مهارات الاختراق، ونحيل في هذا الشأن إلى ما سبق تناوله في موضوع المجرم المعلوماتي.

ومن التطبيقات القضائية على هذه الجريمة؛ القضية رقم 3/ق/2004 الدائرة الجزائية – المحكمة الابتدائية مسقط – سلطنة عمان ، وتتلخص وقائع القضية في قيام عدد من الأشخاص بالاستيلاء غير المشروع على بيانات ومعلومات خاصة بالبطاقات المالية لعملاء بعض البنوك العاملة بسلطنة عمان وذلك باستخدامهم لأجهزة حاسب آلي وبعض الأجهزة المساعدة .وقد تم تنفيذ الجريمة على ثلاثة مراحل وهي :

1- قيام المتهمين بوضع كاميرات فيديو صغيرة جدا موضوعه داخل لوح بلاستيكي يوضع أعلى لوحة المفاتيح الموجودة بجهاز الصرف الآلي وذلك لتصوير العميل وهو يقوم بإدخال الرقم السري

2- وضع جهاز قارئ بطاقات داخل الفتحة الخاصة بالبطاقات وذلك بهدف قراءة البيانات الخاصة ببطاقة العميل وذلك بعد أن يتم تحديد أجهزة الصراف الآلي الذي من خلاله يتم الحصول على تلك البيانات

3- وأخيراً يقوم المجرمون بتفريغ البيانات المسجلة في تلك الأجهزة وإرسالها إلى إحدى الدول حيث يتم تصنيع بطاقات صرف آلي بنفس البيانات والأرقام السرية ليتم بعد ذلك استخدامها لسحب أموال العملاء الضحايا.

وقد وجهت سلطة الاتهام إلى المتهمين جنحتي استخدام الحاسب الآلي عمدا في الالتقاط غير المشروع للمعلومات، والاستيلاء على نحو غير مشروع على بيانات تخص الغير. وطالبت بإدانتهم ومعاقبتهم بموجب المادتين (276) مكرر والمادة (276مكرر 1) من قانون الجزاء العُماني، كما طالبت بتشديد العقوبة بحق المتهمين كونهم من مستخدمي الحاسب الآلي وذلك عملا بنص المادة (276 مكرر 2) من ذات القانون.وقد انتهت الدائرة الجزائية بالمحكمة

الابتدائية، إلى أن الأفعال المرتكبة من قبل المتهمين كانت تنفيذاً لخطة إجرامية واحدة وبالتالي فهي تشكل تعدداً معنويا وقضت بعقوبة الوصف الأشد عملا بنص المادة (31) من قانون الجزاء العماني ، أما فيما يتعلق بتشديد العقوبة فذهبت المحكمة إلى أن لفظ (مستخدمي) الواردة في (المادة 276مكرر 1) تشمل مدلولاً أوسع من لفظ (استخدام) ، فالأولى تعني التمرس والاحتراف وتعدد الاستخدام وكثرته ، بينما مدلول الثانية هو استخدام الحاسب الآلي على نحو عابر دون الاحتراف ، وبما أن سلطة الاتهام لم تقدم لها ما يفيد اعتياد المتهمين على استخدام الحاسب الآلي فإنها تستبعد استعمال (المادة 276مكرر 1) بحق المتهمين. وحكمت بإدانتهم جميعا بتهمة استخدام الحاسب الآلي عمدا في الالتقاط غير المشروع للمعلومات والاستيلاء على نحو غير مشروع على بيانات تخص الغير وقضت بسجنهم لمدة سنتين مع طردهم من البلاد مؤبدا بعد انتهاء فترة عقوبتهم ومصادرة الأدوات المضبوطة التي كانت بحوزتهم[1].

---

(1) نقلاً عن – د. حسين بن سعيد الغافري - الجرائم الافتراضية وجهود سلطنة عمان التشريعية في مواجهتها - المؤتمر العلمي الأول (الجوانب القانونية للمعلوماتية بين النظرية والتطبيق) كلية الحقوق – جامعة السلطان قابوس في الفترة من 13 – 2011/3/14 م- ص 12

الفرع الرابع

موقف المشرع البحريني من جريمة الاعتراض غير القانوني

تنص المادة (26) من دستور مملكة البحرين لسنة 1973 المعدل سنة 2002 على أن (حرية المراسلة البريدية والبرقية والهاتفية والإلكترونية مصونة، وسريتها مكفولة، فلا يجوز مراقبة المراسلات أو إفشاء سريتها إلا في الضرورات التي يبينها القانون، ووفقا للإجراءات والضمانات المنصوص عليها فيه.)

ولقد بينت المذكرة التفسيرية لدستور مملكة البحرين لسنة 1973 المعدل سنة 2002 في معرض تبرير التعديلات التي أجريت على المادة 26 من الدستور الهدف من هذه المادة وهو أنه (أمام التقدم العلمي الذي سيطرت فيه الثورة المعلوماتية والأجهزة الإلكترونية الحديثة على المجتمعات المعاصرة، ونظرا إلى ما يمثله ذلك من خطورة على حرمة الحياة الخاصة للمواطنين، عدلت هذه المادة لتضيف إلى وسائل حماية الحياة الخاصة عدم جواز مراقبة المراسلات الإلكترونية إلا بضوابط معينة، شأنها في ذلك شأن المراسلات البريدية والبرقية والهاتفية)

بالرجوع إلى المادة (372) من قانون العقوبات البحريني والتي تنص على أنه (يعاقب بالغرامة التي لا تجاوز عشرين دينارا من فض رسالة أو برقية بغير رضا من أرسلت إليه أو استرق السمع في مكالمة تليفونية. ويعاقب الجاني بالحبس مدة لا تزيد على ستة أشهر أو بالغرامة التي لا تجاوز خمسين دينارا إذا أفشى الرسالة أو البرقية أو المكالمة لغير من وجهت إليه ودون إذنه متى كان من شأن ذلك إلحاق ضرر بالغير.) ، نلاحظ أنه على الرغم مما تكفله هذه المادة من حماية للحياة الخاصة وصون حرمة المراسلات والمكالمات الهاتفية من الاعتداء على مضمونها وإفشاء محتواها في غير الأحوال المقررة قانوناً، إلا أن تلك الحماية قاصرة على الوسائل التقليدية في المراسلات والمكالمات التليفونية، دون أن تشمل المراسلات الإلكترونية المنصوص عليها في الدستور مثل البريد

الإلكتروني والتصنت على المعلومات المنقولة عبر الشبكات، والقول بغير ذلك يتعارض مع مبدأ الشرعية الجنائية الذي يقضي بأنه لا جريمة ولا عقوبة إلا بنص، وبأنه لا يجوز القياس في مجال التجريم والعقاب، ولا التوسع في تفسير النصوص الجزائية.

ولقد تلافى المشرع البحريني هذا النقص بالنصوص العقابية التي تضمنها المرسوم بقانون رقم (48) لسنة 2002 بإصدار قانون الاتصالات التي اشتملت على صور حماية المراسلات الإلكترونية والتي تشمل جريمة الاعتراض غير القانوني للبيانات والمعلومات وبيان ذلك كالآتي:

أ تنص المادة (73) على أنه (مع عدم الإخلال بأية عقوبة أشد ينص عليها قانون العقوبات أو أي قانون آالعقوبتين: يعاقب بالحبس مدة لا تزيد على ثلاثة أشهر وبغرامة لا تجاوز خمسين ألف دينار أو بإحدى هاتين العقوبتين :1- كل من أعاق أو حور أو شطب محتويات رسالة بواسطة أجهزة أو شبكة اتصالات أو حرض غيره على القيام بهذا العمل...)

ب- تنص المادة (75) على أنه (مع عدم الإخلال بأية عقوبة أشد ينص عليها قانون العقوبات أو أي قانون آخر, يعاقب بالغرامة التي لا تجاوز عشرة آلاف دينار كل من استخدم أجهزة أو شبكة الاتصالات بقصد :...2- التصنت على أو إفشاء سرية أية مكالمات أو بيانات تتعلق بمضمون أية رسالة أو بمرسلها أو بالمرسل إليه, ما لم يكن التصنت أو الإفشاء بموجب إذن من النيابة العامة أو أمر صادر من المحكمة المختصة.)

وبهذا تكون النصوص السابقة قد استوعبت التعديلات التي جاءت بالمادة (26) من دستور مملكة البحرين بشمول المراسلات الإلكترونية بالحماية الجنائية، ومن جهة آخرى تكون شملت معظم صور جريمة الاعتراض القانوني للبيانات والمعلومات الإلكترونية، وإن كانت بحاجة إلى إضافة صورة تسجيل البيانات والمعلومات لذا اقترح على المشرع البحريني تعديل المادة (75) من قانون الاتصالات سالفة البيان بحيث تشمل هذه الصورة.

المطلب الثالث

موقف التشريع الإسلامي من حماية سرية المعلومات

يتناول هذا المطلب موقف التشريع الإسلامي من حماية سرية المعلومات باعتباره أحد مصادر التشريع الرئيسة وفقا لأحكام دستور مملكة البحرين وسائر الدول العربية والإسلامية، سواء وهي في مرحلة سكونها بتجريم الدخول غير المصرح به إلى النظام المعلوماتي، أو في مرحلة حركتها وتنقلها من نظام معلوماتي لآخر ومن مكان لآخر وذلك بتجريم الاعتراض أو الالتقاط غير القانوني للمعلومات والبيانات.

لقد شهد الله تعالى لذاته العليا بإتقان صنع كل شيء وليس هناك أعظم من الله شاهدا، فصدق الله العظيم بقوله تعالى (صُنْعَ اللهِ الَّذِي أَتْقَنَ كُلَّ شَيْءٍ إنه خَبِيرٌ بِمَا تَفْعَلُونَ) (88 - النمل). والشريعة الإسلامية وما حوته من أحكام الله عز وجل جاءت محكمة لا نقص فيها ولا عوجا، قال تعالى (الْحَمْدُ للهِ الَّذِي أَنْزَلَ عَلَى عَبْدِهِ الْكِتَابَ وَلَمْ يَجْعَلْ لَهُ عِوَجًا) (1 - الكهف).وهي صالحة لكل زمان (حاضراً وماضياً ومستقبلاً) ولكل مكان، ولكل الأجناس على اختلاف عاداتهم وطبائعهم، وتقدمهم وتطورهم. فالشريعة الإسلامية جامعة تجمع بين دفتيها حكم كل حالة، ومانعة لا تخرج منها حالة، تشمل بأحكامها جميع صور سلوك البشر ومعاملاتهم وعلاقاتهم، الدينية والدنيوية بما فيها الاجتماعية والاقتصادية والسياسية، فهي صنع الله الذي أتقن صنع كل شيء.[1]

ولقد جبل الإنسان على حب الاستطلاع والاستكشاف والبحث عن كل ما هو مجهول بالنسبة له واستكشاف الأسرار والبحث في خفايا الأمور، فهي غريزة بداخله يبدأ ممارستها من صغره، فالطفل لا يكف عن محاولة استكشاف محيطه. ولقد كانت هذه الغريزة سببا رئيسا فيما توصل إليه من تقدم وتتطور،

---

(1) عبدالقادر عودة – التشريع الجنائي الإسلامي مقارنا بالقانون الوضعي – دار الطباعة الحديثة - 1984 – ج1 – ص15-18

وهو أمر يقره الدين والقانون، فالقاعدة أن حرية البحث والمعرفة مكفولة، ولكن هذه الحرية ليست مطلقة وإنما تحكمها ضوابط تقرها كل من الشريعة والقانون لصالح باقي أفراد المجتمع. فحرية الشخص تنتهي عند بدء حرية الآخرين، وعليه فإذا كان من حق الفرد البحث عن المعلومة إلا أنه يتعين عليه أن يمارس هذا الحق وفقا لضوابطه ووسائله المشروعة، وبما لا يمس حقوق ومصالح غيره من أفراد المجتمع في حماية المعلومات والبيانات الخاصة بهم من أي اعتداء يمس بسلامتها أو سريتها.

ومن منطلق ما سبق، وبمطالعة أحكام الشريعة الإسلامية، نلاحظ أنها قد أقرت الحق في الخصوصية وحماية السرية بشكل عام ، حتى يأمن كل فرد على سره، ونستنبط ذلك من قوله تعالى (يَا أَيُّهَا الَّذِينَ آمَنُوا اجْتَنِبُوا كَثِيرًا مِنَ الظَّنِّ إِنَّ بَعْضَ الظَّنِّ إِثْمٌ وَلَا تَجَسَّسُوا)(12- الحجرات)

وعن أبي هريرة رضي الله عنه قال: قال رسول الله صلى الله عليه وسلم " :إياكم والظن؛ فإن الظن أكذب الحديث، ولا تجسسوا ولا تحسسوا ولا تنافسوا ولا تحاسدوا ولا تباغضوا ولا تدابروا، وكونوا عباد الله إخواناً") رواه البخاري[1]

وقد عرف الإمام الأوزاعي[2] التجسس (بأنه البحث عن الشيء. والتحسس: الاستماع إلى حديث القوم وهم له كارهون، أو يتسمع على أبوابهم[3].

وفي تعريف أكثر تفصيلا ، (التجسس محاولة العلم بالشيء بطريقة سرية لا

---

(1) الحافظ أحمد بن حجر العسقلاني – فتح الباري بشرح صحيح البخاري – دار الفكر للطباعة والنشر والتوزيع – بيروت 1993 - ج12 – ص106

(2) هو أبو عمرو عبد الرحمن بن عمرو بن يُحْمِد الأَوْزَاعِيُّ ، "الأوزاع قرية بدمشق وقد وُلِد في بَعْلَبَك سنة 88هـ/ 707م، ونشأ في البقاع، وسكن بيروت.ويُعَدُّ الإمامُ الأَوْزَاعِيُّ أحد الفُقَهَاءِ الأعلام الذين أثَّرُوا في مَسِيرَةِ الفِقْهِ الإِسْلاَمِيِّ، خَاصَّةً في بلادِ الشَّامِ والأندلس. قال الحافظ ابن كثير: "وقد بقي أهل دمشق وما حولها من البلاد على مذهبه نحوًا من مائتين وعشرين سنة "- راجع http //www islamstory com

(3) الإمام الحافظ أبي الفداء إسماعيل إبن كثير – تفسير القرآن العظيم – دار الجيل – بيروت – ج4 (سنة النشر غير مذكورة) – ص 214- 215

يفطن لها، أو البحث عما يكتم من الأمور، وقيل : هـو والتحسـس - بالحـاء- بمعنـى واحـد، وقيل : إن الثاني هو طلب الأخبار والبحث عنها، وقيل : هو تطلبهـا لنفسـه ، أمـا التجسـس فهو طلبها لغيره)[1]

ويقول الإمـام الطـبري[2]: { وَلا تَجَسَّسُـوا } يقـول: أي لا يتتبـع بعضـكم عـورة أخيـه ولا يبحث عن سـرائره، يبتغي بذلك الظهور على عيوبه.)[3]

وبناءً على ما تقدم، فقد نهت الشـريعة الإسـلامية عـن التجسـس والبحـث عـما يكتمـه الشخص من أسـرار، يكره أن يطلع عليها أحد، لما فيه من كشف العورات، ومـا يترتـب عـلى ذلك من ضغينة وبغضاء بين أفراد المجتمع ، وقد نهى رسول اللـه صلى اللـه عليه وسـلم عن تتبع عورات المسلمين فإن من اتبع عوراتهم يتبع اللـه عورته، ومن يتبـع اللـه عورتـه يفضحه في بيته.

وقـد أوردت بالأحاديـث النبويـة الشـريفة صـوراً لانتهـاك الخصوصـية وتتبـع عـورات المسلمين وكشف سترهم وبيان ذلك كالآتي:

الصورة الأول: حالة قيام شخص بانتهاك حرمة بيت شخص آخر بـالنظر مـن نافـذة أو غيرها ليتعرف ما بداخله بغير إذن صاحب المنزل، فقد روي عَنْ أَبِي هُرَيْرَةَ (عَنْ النَّبِيِّ صَـلَّى اللـه عَلَيْهِ وَسَلَّمَ قَالَ مَنْ اطَّلَعَ فِي بَيْتِ قَوْمٍ بِغَيْرِ إِذْنِهِمْ فَقَدْ حَلَّ لَهُمْ أَنْ يَفْقَئُوا عَيْنَهُ)[4]

---

(1)فتاوى دار الإفتاء المصرية – الشيخ عطية صقر - مايو 1997- راجع http://islamport.com

(2)هو محمد بن جرير بن يريد بن كثير بن غالب الطبري رحمه اللـه تعالى، يُكنى بـأبي جعفـر، واتفـق المؤرخـون على أنه لم يكن له ولد يسمى بـجعفر، بل إنه لم يتزوج أصلاً، ولكنه تكنّى التزامًا بآداب الشـرع الحنيف، وُلـد سنة 224هـ/ 839م، وكانت ولادته بآمُل عاصمة إقليم طبرستان .قـال الخطيـب البغـدادي. "اسـتوطن الطـبري بغداد، وأقام بها إلى حين وفاته"

ترك الطبري ثروة عنمية تدل عـلى غـزارة علمـه، وسـعة ثقافتـه، ودقتـه في اختيـار العلـوم الشـرعية والأحكـام المتعلقة بها أشهر مؤلفاته (جامع البيان في تأويـل القـرآن، المعـروف بتفسـير الطـبري، تـاريخ الأمـم والملـوك، المعروف بتاريخ الطبر) .راجع: http://www.islamstory.com/

(3)صالح بن عبداللـه بن حميـد ، عبـدالرحمن بـن محمـد بـن ملـوح - موسـوعة نضرة النعـيم في مكـارم أخـلاق الرسول الكريم صلى اللـه عليه وسـلم- دار الوسيلة للنشـر والتوزيـع – جـدة – الطبعـة الأولى 1998 – صـ 4129

(4)الشيخ حسن أيوب – السلوك الاجتماعي في الاسلام – دار السلام للطباعة والنشـر والتوزيع والترجمة – القـاهرة 1996- صـ13

الصورة الثانية : التصنت على حديث الآخرين:

- عَنْ ابْنِ عَبَّاسٍ (عَنْ النَّبِيِّ صَلَّى اللَّهُ عَلَيْهِ وَسَلَّمَ قَالَ مَنْ تَحَلَّمَ بِحُلْمٍ لَمْ يَرَهُ كُلِّفَ أَنْ يَعْقِدَ بَيْنَ شَعِيرَتَيْنِ وَلَنْ يَفْعَلَ وَمَنْ اسْتَمَعَ إِلَى حَدِيثِ قَوْمٍ وَهُمْ لَهُ كَارِهُونَ أو يَفِرُّونَ مِنْهُ صُبَّ فِي أُذُنِهِ الْآنُكُ يَوْمَ الْقِيَامَةِ وَمَنْ صَوَّرَ صُورَةً عُذِّبَ وَكُلِّفَ أَنْ يَنْفُخَ فِيهَا وَلَيْسَ بِنَافِخٍ) رواه البخاري[1]

ومما تقدم نلاحظ أن النص على تحريم التجسس بقوله تعالى (ولا تجسسوا) جاء عاما، ليشمل كافة صور السلوك - بالتعبير الجنائي - التي تشكل انتهاكا لحق الفرد في الخصوصية ويمكن القياس على الصور السابق بيانها ، صورة آخرى وهي التجسس أو المساس بسرية المعلومات التي يكره أن يطلع عليه غيره دون إذنه، ونستند في ذلك إلى أن عمومية النص تشمل أيضا المحل الذي ينصب عليه فعل التجسس. كما يلاحظ أن الصورتين السابقتين تقابلان في نطاق الجرائم المعلوماتية جريمتي الوصول أو الإطلاع غير المصرح به على المعلومات، وكذلك الاعتراض أو الالتقاط غير القانوني أو التصنت على المعلومات، وذلك إن دل على شيء دل على ما سبق الإشارة إليه من أن الشريعة الإسلامية جامعة لكل الأحكام باختلاف الزمان والمكان.

ومن الصور الآخرى لحماية الخصوصية والتي يمكن القياس عليها في مجال بحثنا وهو حماية سرية المعلومات قوله تعالى (يَا أَيُّهَا الَّذِينَ آمَنُوا لَا تَدْخُلُوا بُيُوتًا غَيْرَ بُيُوتِكُمْ حَتَّى تَسْتَأْنِسُوا وَتُسَلِّمُوا عَلَى أَهْلِهَا ذَلِكُمْ خَيْرٌ لَكُمْ لَعَلَّكُمْ تَذَكَّرُونَ (27) فَإِنْ لَمْ تَجِدُوا فِيهَا أَحَدًا فَلَا تَدْخُلُوهَا حَتَّى يُؤْذَنَ لَكُمْ وَإِنْ قِيلَ لَكُمُ ارْجِعُوا فَارْجِعُوا هُوَ أَزْكَى لَكُمْ وَاللَّهُ بِمَا تَعْمَلُونَ عَلِيمٌ)(28- النور)

إذاً فإن الشريعة الإسلامية قد أحاطت سرية المعلومات بحماية شاملة، سواء من حيث الاطلاع أو الوصول غير المصرح به إلى المعلومات، أو التنصت أو التقاطها أو اعتراضها، وذلك على النحو السالف بيانه.

---

(1) الحافظ أحمد بن حجر العسقلاني – مرجع سابق – صـ 465

المطلب الرابع

الشـروع في الجرائم الماسة بسـرية المعلومات الإلكترونية

تناولت المادة (11) من اتفاقية بودابست المتعلقة بالجريمة الإلكترونية (الشـروع) حيث نصت على أنه (يجب على كل طرف أن يتبنى الإجراءات التشـريعية، وأية إجـراءات آخـرى يرى أنها ضرورية لتجريم، وفقا لقانونه الداخلي- كل شـروع عمدي لارتكاب إحدى الجرائم المشار إليها في المواد 3 -5 -7-8-9(فقرة 1- أ))

كما عاقب المشـرع الفرنسي في القـانون رقـم (19) لسـنة 1988المتعلـق بجـرائم الغـش المعلوماتي المعدل في عام 1994 على الشـروع في هذه الجرائم بنفس عقوبة الجريمـة التامـة بموجب الفقـرة السـابعة مـن المـادة 462، ويـرى الـبعض أن مسـاواة المشـرع الفـرنسي في العقاب بين الشـروع في الجريمـة المعلوماتيـة والعقوبـة المقـررة للجريمـة التامـة،ترجع إلى خصوصية الجريمة المعلوماتية مما استدعى المشـرع الخروج على القواعد العامة التـي تقـرر عقوبة أقل للشـروع من تلك المقررة في حالة تمام الجريمة[1].

وقد أخذ بذات الاتجاه المشـرع التـونسي حيـث تـنص المـادة (199 مكـرر) مـن قـانون العقوبات لسنة 1913 المعـدل بالقـانون رقـم 89 لسـنة 1999 (المجلـة الجزائيـة) عـلى أنـه (يعاقب بالسجن من شهرين إلى عام وبخطية قدرها ألف دينار أو بإحدى هاتين العقـوبتين فقط، كل مـن ينفـذ أو يبقـى بصـفة غـير شـرعية بكامـل أو بجـزء مـن نظـام البرمجيـات والبيانات المعلوماتية.وترفع العقوبة إلى عامين سجنا والخطية إلى ألفـي دينـار إذا نـتج عـن ذلك ولو عن غـير قصـد إفسـاد أو تـدمير البيانـات الموجـودة بالنظـام المـذكور....والمحاولـة موجبة للعقاب.)، وكذلك فعل قـانون العقوبـات الجزائـري حيـث تـنص المـادة 394 مكـرر عـلى أنـه (يعاقـب بـالحبس مـن ثلاثـة (3) أشـهر إلى سـنة (1) وبغرامـة مـن 50.000 د ج إلى 100.000 د ج كـل مـن يـدخل أو يبقـى عـن طريـق الغـش في كـل أو جـزء مـن

---

(1) د. عمر أبو الفتوح عبدالعظيم الحمامي – مرجع سابق – صـ 1011-1012

منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك...)[1].

بينما عاقب قانون مكافحة جرائم تقنية المعلومات العماني لسنة 2011 على الشروع في الجرائم المعلوماتية بنصف الحد الأعلى للعقوبة المقررة للجريمة حيث تنص المادة (30) منه على أنه (يعاقب بنصف الحد الأعلى للعقوبة المقررة قانوناً للجريمة على الشروع في ارتكاب إحدى الجرائم المنصوص عليها في هذا القانون). وبذات الاتجاه أخذ نظام مكافحة المعلومات السعودي لعام 2007 في المادة العاشرة منه.

بعد تناول موقف التشريعات العقابية من العقوبة على الشروع في الجرائم المعلوماتية على النحو السالف بيانه، سنتناول في هذا المطلب موضوع البدء في التنفيذ في الجرائم الماسة بسرية المعلومات الإلكترونية وبعض الإشكاليات التي تحيط به، حيث يعد التمييز بين الأعمال التي تعد تحضيرا وتلك التي تعد بدء في تنفيذ أهم إشكاليات الشروع في تلك الجرائم.

ويقتضي تحديد مدلول البدء في تنفيذ الجرائم الماسة بسرية المعلومات الإلكترونية بيان ماهية الشروع وموضع البدء في التنفيذ من مراحل ارتكاب الجريمة، وتحديد المرحلة التي يتدخل فيها القانون بالعقاب وتمييزها عن المراحل السابقة عليها التي لا يقرر فيها عقاباً.

---

(1) وتجدر الإشارة إلى أن قانون العقوبات التونسي والجزائري من التشريعات التي تستخدم مصطلح (المحاولة) للتعبير عن الشروع.

الفرع الأول

مفهوم الشـروع

يتنازع الشـروع من حيث التعريف والتجريم مذهبان وهما[1]:

أولا: المذهب المادي والذي يشترط في الشــروع أن يبـدأ الجـاني بارتكـاب أحـد الأفعـال المكونة للركن المادي للجريمة، ولا يعتد بما يسبق ذلك من أفعـال حيـث يـدخلها في مرحلـة التحضير للجريمة.

ثانياً: المذهب الشخصي يعتد بالنية الإجرامية أكثر من اعتداد المذهب المادي بها، ويعـد شـروعا وفقا لهذا المذهب ارتكاب الفاعل فعلا معينـا بنيـة ارتكـاب فعـل لاحـق لـه يـؤدي مباشـرة إلى تحقيق النتيجة الإجرامية التـي يسـتهدفها، ولا يشـترط وفقـا لهـذا المـذهب أن يكون الفعل الذي ارتكبه الفاعل يدخل مباشـرة في الأفعال المكونـة للـركن المـادي للجريمـة طالما أنه سيؤدي مباشـرة إلى تحقيق النتيجة الإجرامية التي يريدها.

ولقد تبنى المشـرع البحريني المذهب الشخصي في تعريفه للشـروع حيـث تـنص المـادة (36) من قانون العقوبات البحريني بأن الشـروع هو (أن يأتي الفاعل بقصد ارتكابهـا عمـلا من شأنه أن يؤدي مباشـرة إلى اقترافها وذلك إذا لم تتم .

ولا يعد شـروعا مجرد العزم على ارتكاب الجريمة أو الأعمال التحضـيرية لهـا أو محاولـة ارتكابها .)

وكذلك المشـرع المصري، حيث عرفت المادة (45) من قانون العقوبـات الشــروع بأنـه (البدء في تنفيذ فعل بقصد ارتكاب جناية أو جنحة إذا أوقف أو خاب أثره لأسـباب لا دخـل لإرادة الفاعـل فيهـا. ولا يعتـبر شــروعا في الجنايـة أو الجنحـة مجـرد العـزم عـلى ارتكابهـا والأعمال التحضيرية لذلك)

---

(1) د.ضاري خيل محمود – الشـروع في الجريمة في قانون العقوبات البحريني المقارن فقها وقضـاء – مجلـة كليـة الحقوق – جامعة البحرين – العدد الخامس مكرر 2005 – صـ 12 - 13

الفرع الثاني

موضع البدء في التنفيذ من مراحل ارتكاب الجريمة

لا تقع الجرائم عادة مرة واحدة و لكنها في معظم الأحيان تمر بعدة مراحل تتمثل في التفكير لارتكاب الجريمة ثم الإعداد و التحضير لها ثم البدء في تنفيذها، والمرحلة الأخيرة التنفيذ التام أو الكامل للجريمة، وستقتصر دراستنا على المراحل السابقة على التنفيذ الكامل للجريمة لخروج تلك المرحلة عن مجال دراستنا في هذا الموضع.

أولا: مرحلة التفكير والعزم والتصميم:

مرحلة التفكير في الجريمة هي مرحلة النشاط الذهني والنفسي الذي يدور في داخل الجاني حيث تولد فكرة ارتكاب الجريمة في ذهنه ويبدأ فيها الموازنة بين دوافع الإقدام على الجريمة ودوافع الإحجام عن اقترافها وبعدها يعقد الجاني العزم والتصميم على ارتكاب الجريمة.

والقاعدة أنه لا تجريم ولا عقاب على ما يدور داخل النفس مهما ظهر العزم عليها قاطعا[1]، ولا خلاف في ذلك بين التشريعات أو الفقهاء، ذلك أن القانون يشترط لوجود الجريمة أن يتحقق فيها كيان مادي ملموس يحدث أثرا أو تغيرا يحرمه القانون، فضلا عن أن عدم شمول التفكير بالتجريم يجد أساسه في السياسة العقابية وهي التشجيع على العدول والرجوع عن ارتكاب الجريمة.

ثانياً: مرحلة الأعمال التحضيرية:

بعد تخطي مرحلة التفكير في الإقدام على الجريمة أو الإحجام عن اقترافها،وبعد عقد العزم والتصميم على ارتكاب الجريمة، يبدأ الجاني الاستعداد لها بأعمال تحضيرية لتنفيذ الجريمة وتحديد إستراتيجية وآلية ووسائل التنفيذ، كأن يقوم الجاني في سبيل ارتكاب جريمة معلوماتية بشراء أو تصميم برامج أو الفيروسات التي تمكنه من اختراق ودخول نظم المعلومات الإلكترونية

---

(1) أ.د أحمد عوض بلال – مبادئ قانون العقوبات المصري –القسم العام – دار النهضة العربية- القاهرة 2006- صـ 324-325

والوصول إلى المعلومات المخزنة بداخلها، أو شراء أو إعداد معدات وأدوات اعتراض البيانات والتقاطها وتسجيلها والتصنت عليها.

والأصل أن المشرع لا يعاقب على الأعمال التحضيرية لارتكاب الجريمة، ولا يعتبرها شروعا فيها، ويؤسس ذلك على أن تلك الأعمال ليست قاطعة الدلالة على النية الإجرامية [(1)]إضافة إلى أن عدم العقاب على الأعمال التحضيرية تتفق مع السياسة العقابية كحافز لدى الجاني للعدول عن مشروعه الإجرامي[(2)]. وقد استبعد المشرع البحريني مرحلة الأعمال التحضيرية من نطاق العقاب حيث تنص المادة(36) من قانون العقوبات على أنه (... ولا يعد شروعا مجرد العزم على ارتكاب الجريمة أو الأعمال التحضيرية لها أو محاولة ارتكابها.)

ولكن قد يشكل العمل التحضيري جريمة مستقلة في حد ذاته حيث قد يرى المشرع أن هذا العمل يمثل خطورة على المجتمع والحق المحمي، فيجعل منه المشرع جريمة مستقلة عن الجريمة التي يتم التحضير لها. مثل حيازة سلاح بدون ترخيص أو تقليد المفاتيح[(3)].

ومن الأعمال التحضيرية التي تشكل جريمة في حد ذاتها التي جرمها المشرع البحريني وتتعلق بالتحضير لجريمة الاعتراض غير القانوني للبيانات والمعلومات الإلكترونية تشغيل شبكة اتصالات تستخدم طيفاً ترددياً في المملكة أو تشغيل أو استخدام أية أجهزة اتصالات راديوية متعلقة بهذه الشبكة دون الحصول على ترخيص بذلك من هيئة تنظيم الاتصالات، أو استخدام بوجه غير مشروع أي جهاز اتصالات بقصد إحداث تداخل ضار بأية اتصالات، أو حيازة أجهزة اتصالات غير مرخص بها من هيئة تنظيم الاتصالات، وذلك بموجب المادة (73) من المرسوم بقانون رقم (48) لسنة 2002 بإصدار قانون

---

(1) د. سليمان عبدالمنعم – النظرية العامة لقانون العقوبات – دار الجامعة الجديدة لنشر 2000 - الإسكندرية - صـ 594

(2) د.ضاري خليل محمود – مرجع سابق – صـ 19

(3) د.فوزية عبدالستار - شرح قانون العقوبات – القسم العام – النظرية العامة لجريمة- دار النهضة العربية 1992 القاهرة - صـ288

الاتصالات بدلالة المواد (43)، (49) من ذات القانون.

كما جرم القانون الفرنسي رقم (19) لسنة 1988 الخاص بالجرائم المعلوماتية في المادة (462- 8) الأعمال التحضيرية إذا اتخذت صورة الاتفاق الجنائي من أجل تنفيذ جريمة من الجرائم المنصوص عليها في ذات القانون من المادة (462-2) إلى المادة (462-6) والتي من بينها الجرائم الماسة بسرية المعلومات الإلكترونية المادة (462-2 الخاصة بالدخول والبقاء غير المصرح بهما داخل نظام المعالجة الآلية للبيانات[1].

ثالثا: البدء في التنفيذ:

هو المرحلة التي يصل إليها الجاني بعد قطع أشواطً اتجاه ارتكاب جريمته متجاوزا مراحل التفكير في الجريمة والتحضير لها ، وإذا كان المشرع لم يشمل بالعقاب المراحل السابقة لعدم تشكيلها تهديداً حقيقياً للحقوق المحمية ورغبة منه في فتح المجال للجاني للتراجع والعدول عن جريمته كما سبق الإشارة، فإن وصوله إلى هذه المرحلة – البدء في تنفيذ الجريمة – فإن ذلك يدل على خطورته الإجرامية فضلا عن تشكيله مساساً أو تهديداً حقيقياً للحقوق المحمية، مما يستوجب تتدخل القانون بالعقاب في هذه المرحلة.

وقد اختلف الفقه بشأن وضع معيار لتحديد البدء في التنفيذ، حيث انقسم إلى مذهبين الأول المذهب المادي، والثاني المذهب الشخصي.

أ- **معيار البدء في التنفيذ وفقا للمذهب المادي:**

يعتمد أنصار هذا المذهب على ماديات النشاط الإجرامي لا على مجرد الإرادة الإجرامية، ويقوم البدء في التنفيذ وفقا لهذا المذهب بإتيان فعل من الأفعال المكونة للركن المادي للجريمة وفقا للنموذج المنصوص عليه في نص التجريم، وأن ما يسبق ارتكاب هذا الفعل لا يعد بدءاً في التنفي0ذ ويدخل ضمن المراحل السابقة عليه. ونتيجة للانتقادات التي وجهت إلى هذا المذهب الذي يضيق من

(1) د. عمر أبو الفتوح عبدالعظيم الحمامي – مرجع سابق – صـ1013

نطاق الشروع إلى الحد الذي يهدر مصلحة المجتمع، ذهب بعض فقهاء هذا المذهب إلى أن البدء بالتنفيذ يتحقق إذا انطوى العمل الذي أتاه الجاني في ذاته على احتمال حدوث النتيجة الإجرامية، وذهب البعض الآخر إلى أن البدء في التنفيذ يتحقق بإتيان الجاني فضلا عن أفعال الركن المادي للجريمة أي فعل يعد ظرفا مشدداً لعقوبتها [1]

ب- معيار البدء في التنفيذ وفقا للمذهب الشخصي:

يعول أنصار هذا المذهب الشخصي على نية الجاني وشخصيته باعتبارها مصدر الخطورة الإجرامية، ويعد بدءاً في التنفيذ وفقا لهذا المذهب إذا أتى الجاني أفعال تعبر عن خطورة شخصية الجاني ونيته. وقد تأثر هذا المذهب بالمدرسة الوضعية التي ترى أن مركز الثقل في قانون العقوبات هو المجرم لا الجريمة[2].

وقد تعددت الصيغ التي صاغها أنصار هذا المذهب للتعبير عن هذا المعيار، بأن البدء في التنفيذ هو" العمل الذي يكون قريباً من الجريمة بحيث يمكن أن يقال إن الجاني قد أقفل باب الرجوع عنها وتحمل مخاطرها "، أو هو" الفعل الذي يدخل به الجاني في مرحلة العمل على تنفيذ الجريمة بحيث يمكن القول بأنه قد" أحرق سفنه وخطا نحو الجريمة خطوته الحاسمة ."وأقرب الصيغ تعبيراً عن المذهب الشخصي هي التي تحدد البدء في التنفيذ بأنه "العمل الذي يؤدى حالاً ومباشرة إلى الجريمة " ، وتعد الصيغة الأخيرة هي الأرجح والأكثر استخداما من قبل الفقهاء والمشرعين وكذلك القضاء.[3]

ووفقا لهذا المذهب فإنه يشترط أن تتوافر ثلاثة عناصر مجتمعة في الفعل حتى يوصف بالبدء في التنفيذ وهي كالآتي[4]:

1- إتيان الجاني عملاً يخرج عن الركن المادي ولكنه ينطوي على خطورة تهدد الحق المحمي قانوناً.

---

(1) د. أحمد فتحي سرور - الوسيط في قانون العقوبات - دار النهضة العربية - القاهرة 1996 - صـ 303

(2) المرجع نفسه صـ 304

(3) د. سليمان عبدالمنعم - مرجع سابق - صـ 601

(4) د. ضاري خليل محمود - مرجع سابق صـ26 - 27

2- أن يكون من شأن العمل أن يؤدي مباشـرة إلى ارتكاب الجريمة.

3- وجود نية ثابتة ومستمرة لدى الجاني على ارتكاب الجريمة.

وتتجلى أهمية تـوافر تلـك العنـاصر في الفعـل في أنـه لا يمكـن وصـفه بأنـه يـؤدي مباشـرة إلى الجريمة ما لم يكن مقترناً بنيه ثابتة على ارتكاب الجريمة، كما أن نية الفاعل لا توصف بأنها ثابتـة عـلى ارتكـاب الجريمـة مـا لم تقـترن بقيـام الفاعـل بعمـل يـؤدي مباشـرة إلى ارتكاب الجريمة.ولقد تبنت معظـم التشــريعات العربيـة بمـا فيهـا قـانون العقوبات البحريني المذهب الشخصي حيث تنص المادة (36) منه على أن (الشـروع في الجريمة هو أن يأتي الفاعل بقصد ارتكابها عملا من شأنه أن يؤدي مباشـرة إلى اقترافها وذلك إذا لم تتم.)

الفرع الثالث

تحديد البدء في التنفيذ في الجرائم الماسة بسرية المعلومات الإلكترونية

آثار التمييز بين بدء التنفيذ المعاقب عليه والأعمال التحضيرية غير المعاقب عليها إشكالية في نطاق جرائم المعلوماتية.حيث اختلفت الآراء بهذا الشأن، فذهب رأي إلى مد النطاق العقابي ليشمل الأعمال التحضيرية التي تتداخل مع مفهوم الشروع، معللاً ذلك بأن نظرية الشروع لن تثمر في إجراء هذا التمييز. وذهب رأي منهم إلى أن الشروع يبدأ في اللحظة التي يذهب فيها الشخص لتشغيل الجهاز، بينما ذهب رأي آخر إلى أن الشروع هو مقدمة لفعل الجريمة وبالتالي فإن الجزء الأكبر من الأعمال التحضيرية يعد داخلا في نطاق الشروع المعاقب عليه[1]. كما يرى البعض أن إشكالية البدء في التنفيذ في الجرائم المعلوماتية تنبع بوجه عام في تحديد المعيار الذي يمكن الاعتماد عليه بالنسبة لهذه الجرائم. حيث يرون أن المعيار الشخصي لا يمكن الاعتماد عليه، ويعود ذلك إلى وحدة النشاط المادي، فمعظم الجرائم المعلوماتية تتطلب القيام بحركة مادية موحدة جوهرها التعامل مع الحاسب،وعلى هذا النحو يصعب القول بإمكانية تحديد نوعية الجريمة المرتكبة أو المراد ارتكابها، فضلا عن أن إعمال المعيار الشخصي في تحديد الشروع يجعل الأمر أقرب إلى إدانة العمل التحضيري في تلك الجرائم، ويرى أنصار هذا الرأي أن ترجيح المعيار المادي على الشخصي في الجرائم المعلوماتية يجعل الشروع في موقع أفضل عند عقد مقارنة بين الشروع وبين التلبس بالجريمة، وهو بذاته ظرف عيني يرتبط بالواقعة الإجرامية بحيث يقترب الأمر من هذه الزاوية من توصيف الواقعة بذاتية خاصة بها منفصلة عن التلبس ذاته[2].

ولقد ثارت إشكالية تحديد البدء في التنفيذ خلال مناقشات البرلمان الفرنسي

---

(1) د. عمرو ابراهيم الوقاد، الحماية الجنائية للمعلوماتية- بدون جهة أو تاريخ نشر، صـ 119

(2) د.عمر محمد أبوبكر بن يونس – الجرائم الناشئة عن استخدام الإنترنت – دار النهضة العربية - القاهرة - الطبعة الأولى 2004- صـ 277-280

للمواد الخاصة بالجرائم المعلوماتية، وقد أدى النقاش إلى أثارة مسألة هامة وهي مسألة الإثبات، حيث ذكر أحد النواب بأنه يمكن كشف محاولات اختراق الأنظمة بطريقة غير مشروعة من خلال جرائد توجد داخل الأنظمة المعلوماتية، بها ذاكرة تحفظ محاولات الاختراق غير المشروعة، وبناء عليه فإنه تقنيا يمكن كشف محاولات البدء في تنفيذ الجريمة المعلوماتية. غير أنه تصعب التفرقة بين أعمال البدء في التنفيذ والأعمال التحضيرية خاصة في حالات محاولة الدخول عن بعد، وهو ما دفع المشرع الفرنسي إلى تبني مبدأ معاقبة الاتفاق الجنائي بهدف التحضير للجرائم المعلوماتية[1].

ولا تثير جريمتا الدخول غير القانوني المجرد أو البقاء غير القانوني داخل النظام المعلوماتي إشكالية من ناحية الشروع ذلك أن هاتين الجريمتين تعدان من طائفة الجرائم الشكلية التي لا يشترط فيها وقوع نتيجة ولذلك تسمى بجرائم الخطر أو جرائم السلوك، التي لا تحدث بطبيعتها أية نتيجة مادية ضارة، التي يكتفي المشرع لتمام الجريمة تحقق السلوك الإجرامي بغض النظر عن النتائج المتحققة من عدمه، فتتحقق الجريمة بمجرد الدخول العمدي غير القانوني لنظام المعالجة الآلية، أو الإبقاء على الاتصال الذي تم دون قصد في بادئ الأمر. وتبرير ذلك أنه وإن كانت علة التجريم هي حماية المعلومات والبرامج من الوصول إليها بطريق غير مشروع وما قد ينجم عنه من أضرار بهذه المعلومات، إلا أن جريمة الدخول أو البقاء غير القانوني داخل النظام المعلوماتي من الجرائم التي تشكل عدوانا محتملا على الحق، حيث أنه بتحقق الدخول إلى النظام تكون المعلومات والأسرار المخزنة داخلة متاحة للجاني، وتحت تصرفه يتخذ بشأنها ما يريد من الاطلاع عليها أو نسخها أو تدميرها أو إتلاف النظام المعلوماتي ذاته.

ومن جانبي أرى أن تحديد البدء بالتنفيذ في جريمة الدخول غير القانوني

---

(1) قارة آمال - الجريمة المعلوماتية - رسالة ماجيستير - جامعة الجزائر - كلية الحقوق - بن كعنون - السنة الجامعية 2001 /2002

بقصد ارتكاب جريمة آخرى كإتلاف البيانات أو الحصول على بيانات سرية حكومية، وهي جريمة ذات النتيجة التي يتصور فيها الشروع، قد يثير إشكالية كبيرة، تتمثل في وحدة النشاط المادي،بينها وبين جريمة الدخول غير القانوني المجرد وهي جريمة شكلية لا يتصور فيها الشروع ، فالسلوك المادي الذي يأتيه الجاني في سبيل ارتكاب كلا الجريمتين واحد،ولإبراز تلك الإشكالية بشكل أوضح نضرب المثال الآتي:

قام شخص بدون وجه حق أو مسوغ قانوني بالضغط على زر تشغيل جهاز الحاسب وبدأ يحاول تجريب كلمات مرور مختلفة بغية الدخول إلى الجهاز إلا أنه في هذه اللحظة وقبل تمكنه من الدخول، تم ضبطه والإمساك به. السؤال الذي يطرح نفسه هو هل يعد الجاني في هذه الحالة قد شرع في جريمته وبالتالي يستحق العقاب على هذا الأساس؟ أم أنه مازال في مرحلة الأعمال التحضيرية التي لا عقاب عليها؟

للإجابة عن هذا السؤال يجب أن نميز بين حالتين، الأولى إذا كان الجاني يقصد من ارتكاب جريمة الدخول المجرد كما هو الحال بالنسبة لكثير من المراهقين الذين يقدمون على اختراق النظم المعلوماتية بقصد التحدي وإثبات القدرة على اختراق الأنظمة كما سبق الإشارة، أي أن هدفهم مجرد الدخول دون انصراف نيتهم إلى إتلاف المعلومات والبيانات أو اختلاسها. ففي هذه الحالة ووفقا لمفهوم كون جريمة الدخول غير القانوني المجرد جريمة شكلية لا يتصور فيها الشروع، وبالتالي فإن ما يسبق مرحلة تنفيذ الجريمة يعد من قبيل المحاولة أو الأعمال التحضيرية التي لا عقاب عليها.

الحالة الثانية إذا كان الجاني يقصد من دخوله غير القانوني إلى النظام المعلوماتي الحصول على بيانات ومعلومات حكومية أو بنكية سرية، فإن الجريمة في هذه الحالة من الجرائم المادية ذات النتيجة التي يتصور الشروع فيها حيث أن النتيجة تخلفت لسبب خارج عن إرادة الجاني، كما أن الجاني في الحالة التي ضبط عليها وفقا للمذهب الشخصي يكون قد بدأ في ارتكاب جريمته بأن أتى عملا

من شأنه أن يؤدى حالاً ومباشرة إلى الجريمة مستحقا للعقاب المقرر قانونا للشروع في هذه الجريمة.

ومن المثال السابق يتضح أهمية تحديد حالة البدء في تنفيذ جريمة الدخول غير القانوني، نظرا لما قد يترتب على ذلك من نتائج خطرة تتمثل في إفلات مجرم بحجة أنه قصد ارتكاب جريمة الدخول المجرد، أو معاقبة شخص على فعل لم يشمله القانون بالعقاب لأن فعله ما يزال في مرحلة الأعمال التحضيرية غير المعاقب عليها.

لذا نرى أن التمييز بين هاتين الحالتين يخضع للسلطة التقديرية لقاضي الموضوع الذي يمكنه استخلاص نية الجاني من ملابسات الواقعة والظروف المحيطة بها، فمثلا يمكن للقاضي الاستدلال على نية الجاني في الدخول غير القانوني للحاسب الآلي بقصد الحصول على المعلومات ونسخها من خلال أدوات أو وسائط التخزين مثل الأقراص المدمجة CD الخالية، أو ذاكرة متنقلة Flash memory التي تكون بحوزته لحظة ضبطه أثناء محاولته الدخول إلى الحاسب الآلي، حيث يستخلص من حيازته لتلك الوسائط نيته في نسخ ونقل البيانات والمعلومات التي سيتوصل إليها داخل الحاسب الآلي محل الجريمة. أو يستخلص من خلال حيازته لبرامج فيروسات مصممة لتدمير البيانات والمعلومات من أنه يقصد من فعله الدخول بقصد إتلاف تلك البيانات، كما يستخلص تلك النية من النظام المعلوماتي المعتدى عليه مثال النظم الخاصة بالبنوك والشركات والأجهزة الأمنية والحكومية، إذ أنه غالبا ما تكون المعلومات والبيانات المخزنة بها هدفاً للاختلاس أو الإتلاف.

ولذلك، اقترح على المشرع البحريني عند معالجته لجريمة الدخول غير القانوني، ان يشمل بالتجريم مرحلة المحاولة بالنسبة للنظم المعلوماتية الخاصة بالمؤسسات الحكومية والأمنية، والدفاع، بالإضافة النظم المعلوماتية الخاصة بالبنوك والمؤسسات المالية، لتحقيق قدر أكبر من الحماية لتلك النظم التي تتضمن معلومات تهدد أمن واستقرار الدولة من الناحية الأمنية والعسكرية والاقتصادية.

ونقصد بمرحلة المحاولة تلك المرحلة التي تلي مرحلة الأعمال التحضيرية وتسبق البدء بالتنفيذ، وهي مرحلة تكون العناصر المادية في حالة حركة وفاعلية أكثر منها في مرحلة الأعمال التحضيرية تجاه ارتكاب الأفعال المادية المكونة للركن المادي للجريمة، ونظرا لكونها متاخمة لمرحلة الأعمال التحضيرية فإنه غالبا ما تعتبرها التشريعات الجنائية جزءاً من الأعمال التحضيرية، إلا في حالات نادرة وفي الجرائم شديدة الخطورة، منها ما جاء بنص المادة (148) من قانون العقوبات البحريني حيث عاقبت من يحاول بالقوة قلب أو تغيير دستور الدولة أو نظامها الملكي، وكذلك عاقبت المادة (149) من ذات القانون على المحاولة بالقوة احتلال أحد المباني العامة أو المخصصة لمصالح حكومية.والمشرع البحريني عندما جرم المحاولة في المواد السابقة فإنه قصد بها المحاولة كمرحلة سابقة على الشروع ولاحقة للأعمال التحضيرية، نظراً لما تشكله هذه الجرائم من خطر على الأمن الاجتماعي [1]. ولو شاء عكس ذلك لا ستخدم مصطلح الشروع، كأن يقول يعاقب كل من شرع بقلب أو تغيير الدستور أو النظام الملكي، أو يعاقب كل من شرع باحتلال أحد المباني العامة وهكذا، إذ لا يجوز أن ينسب للمشرع عدم الدقة في اختيار واستخدام المصطلحات القانونية، ولا يجوز عد المحاولة جزءاً من الأعمال التحضيرية لأن نطاق التجريم سيشمل حالات بعيدة عن ضرورات التجريم فيدخل فيها حتى التافه من الأقوال أو الأعمال.

كما يمكن الاسترشاد بموقف المشرع المصرى عندما جرم بموجب قانون الأحوال المدنية رقم (143) لسنة 1994 محاولة اختراق سرية بيانات ومعلومات مصلحة الأحوال المدنية، حيث تنص المادة (76) من هذا القانون على أنه (يعاقب بالأشغال الشاقة المؤقتة كل من اخترق أو حاول اختراق سرية البيانات أو المعلومات أو الإحصاءات المجمعة بأية صورة من الصور). ولو أراد المشرع المصرى استخدام لفظ الشروع في هذه الجريمة لفعل ذلك، ولكنه أراد استخدام لفظ المحاولة قاصداً بها المرحلة ما قبل الشروع.

---

(1)د. ضاري خليل محمود – مرجع سابق – صـ 19 -20

الفصل الثاني

مكافحة الجرائم المعلوماتية الماسة بسرية المعلومات الإلكترونية

نتيجة لتداخل العديد من العوامل والأسباب المختلفة، أضحت الجرائم المعلوماتية بشكلٍ عام تشكل خطراً كبيراً يهدد أمن كل من المجتمعات الوطنية، والمجتمع الدولي ككل، وحتى لا ينعم مرتكبي هذه الجرائم بملاذات آمنة نتيجة لضعف التعاون الدولي في مجال مكافحتها، أو القصور أو الفراغ التشريعي على المستوى الوطني في هذا المجال، فمكافحة الجرائم المعلوماتية يتطلب بناء منظومة دفاعية متكاملة قوامها التعاون الدولي والمواجهة التشريعية ويتأتى ذلك من خلال تنسيق الجهود بين مختلف الدول لمكافحة هذا النوع من الجرائم وتعزيزها من خلال وسائل التعاون الدولي المختلفة مثل التعاون القضائي وتسليم المجرمين والعمل على تطوير تلك الوسائل وزيادة فاعليتها ومراجعة التشريعات العقابية على المستوى الوطني وتطويرها أو استحداث تشريعات جديدة تتلاءم مع طبيعة تلك الجرائم، وتكون قادرة على ردع مرتكبيها.

وسنسلط الضوء في هذا الفصل على وسائل التعاون الدولي والإقليمي لمكافحة هذه الجرائم وذلك في المبحث الأول، والجهود التشريعية لمكافحتها في المبحث الثاني.

المبحث الأول

التعاون الدولي والإقليمي لمكافحة الجرائم المعلوماتية

نتيجة للتقدم التكنولوجي ظهر لدينا عالم افتراضي مرادف للعالم الواقعي انتقلت إليه كل عادات وسلوكيات الأفراد فانصبغت بصبغته،بما في ذلك السلوك الإجرامي، وهذا العالم الافتراضي لا يعرف الحدود والتقسيمات الموجودة في العالم الواقعي من دول وقارات وعلى الرغم من إيجابيات ذلك، فإن الجرائم التي تقع في العالم الافتراضي باتت تشكل تحدياً كبيراً لمختلف دول العالم، ذلك أنها عندما ترتكب في العالم الافتراضي فإن آثارها غالباً ما تنتقل إلى عدة دول، وهو ما يثير إشكاليات وتحديات على أرض الواقع أبرزها مبدأ إقليمية القانون، ومبدأ احترام سيادة كل دولة عند مباشرة إجراءات التحقيق من معاينة وجمع الأدلة وفحصها وإجراءات التفتيش وسماع الشهود، وتعقب مرتكبي هذه الجرائم وتقديمهم للمحاكمة،وبالتالي معاقبتهم.

فرسالة واحدة تحتوي على فيروس يستخدم لارتكاب جريمة إتلاف البيانات وهي جريمة معلوماتية يمكن تمريرها من خلال عدد من مزودي خدمات الانترنت في دول يختلف النظام القانوني في كل منها عن الآخر لذا فإنه من الضروري تكاتف جهود الدول من أجل التعاون في مكافحة تلك الجرائم وتسهيل عمليات جمع الأدلة الرقمية وحفظها واتخاذ إجراء سريع بشأنها، نظراً لكونها سريعة الزوال، وسريعة الإتلاف والمحو من قبل الجناة، الأمر الذي جعل الوسائل التقليدية لمعالجة الأمر بطيئة إن لم تكن غير كافية أصلاً، وذلك أن بطء الإجراءات الرسمية أو تعذرها أحياناً قد يؤدي إلى فقدان تلك الأدلة.

وعليه يمكن القول أن الجريمة المعلوماتية بشكل عام من أهم التطبيقات التي تبرز أهمية التعاون الدولي في تقديم المساعدة الأمنية والقضائية، فمكافحة تلك الجريمة يتطلب مساعدة من قبل سلطات البلد الذي انطلقت منه الشرارة الأولى للجريمة (السلوك المادي) ، أو من السلطات في البلد أو البلدان التي عبر

من خلالها النشاط المجرَم وهو في طريقه إلى الهدف، أو حيثما توجد أدلة للجريمة.وفي مثال عملي أهمية التعاون الدولي في مجال مكافحة الجريمة المعلوماتية، قامت المديرية الأمريكية للتفتيش على البريد في عام 1999 بمداهمة مكاتب شركة في ولاية تكساس تدعى (لاندسلايد إنكوربوريتد - Landslide Incorporated) حيث تقوم هذه بتشغيل شبكة لتقديم خدمات استضافة مواقع الإنترنت والتحقق من بطاقات الائتمان لعدد كبير من المواقع التي تقدم بشكل رئيسي مواد إباحية. وكان أكثر النشاطات تحقيقا للأرباح من أنشطة هذه الشركة هو المواقع التي تحتوي على صور إباحية يستغل فيها الأطفال. وقد حقق مالكي هذه الشركة أرباحاً كبيرة من وراء هذا النشاط. وبعد إدانة أصحاب الشركة عام 2001 تم إعطاء نسخة من قاعدة البيانات الخاصة بعملاء الشركة إلى الشرطة البريطانية، وقد ساعدت تلك البيانات على تحديد هوية حوالي 2.300 مشتبه به في بريطانيا يعتقد بأنهم قاموا بدفع أموال للدخول على مواقع تقدم صورا إباحية يستغل فيها الأطفال. وقد بدأت الشرطة البريطانية بإجراء تحقيقات موسعة في هذا الموضوع وكان عدد المشتبه بهم ضخما، ولكن تم إعطاء الأولوية إلى المشتبه فيهم الذين يعتقد أنهم يشكلون خطراً على الأطفال،وتم فحص أجهزة الكومبيوتر الخاصة بهم بعد الحصول على أُذونات التفتيش لكل واحد منهم. ولإثبات الطريقة التي تم بها إدراج أسم الشخص في قاعدة البيانات، كان من الضروري مخاطبة الولايات المتحدة الأمريكية وطلب ذلك منها ، كما تتطلب الأمر أيضاً سفر ضباط بريطانيين لنسخ شبكة أجهزة الكومبيوتر التي استخدمتها شركة (لاندسلايد إنكوربوريتد) لاستعمالها في التحقيقات الجارية في بريطانيا[1].

وقد أكدت اتفاقية مجلس الاتحاد الأوروبي بودابست لسنة 2001 المتعلقة بالجريمة الإلكترونية في المادة (23) على أهمية التعاون الدولي في مجال مكافحة

---

(1) نقلاً عن راسل تاينر - جرائم الإنترنت- التحدي لإنفاذ القانون- برنامج تعزيز حكم القانون في بعض الدول العربية مشروع تحديث النيابات العامة - بحث مقدم بالندوة الإقليمية حول (الجرائم المتصلة بالكومبيوتر) في الفترة 19-20 نيسان / يونيو 2007 المملكة المغربية- ص 89-90.

الجريمة المعلوماتية[1]، كما أكدت الاتفاقية العربية لمكافحة جرائم تقنية المعلومات المبرمة في 21 ديسمبر 2010[2] على أهمية التعاون الدولي في سبيل مكافحة الجريمة المعلوماتية، حيث تنص المادة (32) منها على أنه (1- على جميع الدول الأطراف تبادل المساعدة فيما بينها بأقصى مدى ممكن لغايات التحقيقات أو الإجراءات المتعلقة بجرائم معلومات وتقنية المعلومات أو لجمع الأدلة الإلكترونية في الجرائم..)

وبعد استعراض أهمية التعاون الدولي في مكافحة الجريمة المعلوماتية على النحو المتقدم، سنتناول فيما يلي أهم صور ومجالات هذا التعاون، مع تسليط الضوء على مجالات التعاون التي تستلزمها طبيعة الجرائم المعلوماتية.

---

(1) تنص المادة (23) على أنه (يجب الأطراف أن تتعاون، مع بعضها البعض وفقاً لأحكام هذا الفصل، في تطبيق الأصول الدولية المتصلة بالتعاون الدولي في المواد الجنائية، والاتفاقيات المعتمدة على التشريعات المتماثلة أو النظيرة والقوانين المحلية،إلى أوسع نطاق ممكن لأغراض التنقيب والتحري أو الإجراءات الجنائية المتعلقة بالجرائم الجنائية المرتبطة بنظم وبيانات معلوماتية أو لجمع أدلة ذات شكل إلكتروني للجريمة الجنائية.) - راجع د. هلالي عبداللاه أحمد - كيفية المواجهة التشريعية لجرائم المعلوماتية في النظام البحريني على ضوء اتفاقية بودابست - دار النهضة العربية 2011- القاهرة - صـ 241- 243

(2) نص الاتفاقية منشور على الموقع الإلكتروني لجامعة الدول العربية www.arableagueonline.org

المطلب الأول

جهود أجهزة مكافحة الجرائم الدولية والإقليمية في مجال مواجهة جرائم المعلوماتية

لم يعد الإنترنت وشبكات المعلومات مناطق يصعب فيها تطبيق القانون،حيث يتصور الكثيرون أن هناك غياباً للمراقبة على الشبكات، وأن قدرة المستخدمين على إخفاء هويتهم عن طريق تشفير التوقيعات الخاصة بهم تصعب من مهام الشرطة في تحديد شخصية وملاحقة مرتكب الأفعال المجرَّمة في هذا العالم الافتراضي. فالأفعال المجرَّمة التي ترتكب في داخل الحدود الجغرافية للدولة، دون أن يمتد أثرها إلى خارجها، يستطيع المحققون أن يتعاملوا معها دون مصاعب أو تعقيدات في غالب الأحيان.وأن عدم معرفة شخصية الفاعل الحقيقي مصدر الفعل غير المشروع هو أمر نسبي، إذ لا يوجد تجهيل بالمعنى المتصور بالنسبة لشبكة المعلومات إذ غالباً ما يترك الفاعل آثاراً أثناء تنقله في شبكة المعلومات تمكن المحققين من الوصول إليه[1].

علماً بأن الطابع الدولي للجرائم المعلوماتية وما تتسم به كونها جرائم عابرة للحدود، قد شكل تحدياً أمام أجهزة الشرطة عند قيامها بمهامها كونها تصطدم بمبدأ احترام سيادة الدول، وهو ما يتطلب تعاوناً دولياً بين أجهزة الشرطة في مختلف الدول وتنسيق الاتصال بينها في سبيل تسهيل عملية تعقب مرتكبي هذه الجرائم وإلقاء القبض عليهم ومعاقبتهم، ويمكن أن يتحقق ذلك إما من خلال الاتصال المباشر بين الدولتين أو الدول ذات العلاقة بالجريمة المعلوماتية ، أو عن طريق المنظمات والهيئات الدولية والإقليمية المتخصصة في مجال مكافحة الجريمة. ففي يونيو 2009 ومن خلال عملية شاركت فيها أجهزة الشرطة الخاصة بأربعة دول مجتمعة وهي السويد، والدنمارك، وفنلندا، والنرويج،

---

(1)أ.د. صالح أحمد البربري- بحث بعنوان دور الشرطة في مكافحة جرائم الإنترنت في إطار الاتفاقية الأوروبية الموقعة في بودابست في 2001/11/23 – دون تاريخ نشر – صـ 4 منشور على الموقع الإلكتروني الدليل الإلكتروني للقانون العربيwww.arablawinfo.com

استهدفت مجموعة تطلق على نفسها اسم (محاربي شمال أوروبا الفايكنغ) وهي عبارة عن مجموعة من مجرمي دعارة الأطفال تعمل من خلال الإنترنت , وقد تمكنت هذه المجموعة من إيقاع حوالي ثمانين شخصا في شباكها، وكانت تقوم بتبادل صور جنسية للأطفال على الإنترنت، بالإضافة إلى أنهم كانوا يقومون بتصوير عمليات اعتداء جنسي على ضحاياهم،وقد استغرق التحضير لعملية ضبط هذه المجموعة عدة أشهر.[1]

وتبرز أهمية جهود المنظمات والهيئات في الدعم والمساندة التي تقدمها للدول الأعضاء بها في مجالات التحقيقات المتعلقة بالجرائم المعلوماتية،وتعقب وملاحقة المجرمين وكشف هوياتهم، وجمع الأدلة الرقمية المتعلقة بتلك الجرائم والتي تتطلب مهارة وتقنيات عالية للتعامل معها سواء في تحليلها أو حفظها نظرا لما تتميز به من سرعة الزوال، وهي أمور قد يتعذر على دولة لا تملك من البنية التحتية والأساسية الإلكترونية ولا الكوادر البشرية المؤهلة فنية وتقنية للتحقيق في الجرائم المعلوماتية ما يمكنها من التصدي لأخطار تلك الجرائم مما يجعلها مرتعاً لمجرمي المعلومات وصيداً سهلا لهم.

---

(1) http://arabic.euronews.net/2009/06/16/child-porn-ring-smashed-in-raids/

الفرع الأول

جهود الأجهزة الدولية لمكافحة الجرائم

في مجال مواجهة الجرائم المعلوماتية

نتناول في هذا الفرع جهود المنظمة الدولية للشرطة الجنائية" الإنتربول و شبكة المعلومات التابعة لمجموعة دول الثمانية في مكافحة الجرائم بوجه عام والجرائم المعلوماتية بوجه خاص وذلك على النحو الأتي

أولا: جهود المنظمة الدولية للشرطة الجنائية" الإنتربول"[1] في مجال مواجهة الجرائم المعلوماتية

تسعى منظمة (الإنتربول) إلى الوصل بين أجهزة الشرطة لجعل العالم أكثر أمانا، وتشجيع التعاون بين أجهزة الشرطة في الدول الأطراف وعلى نحو فعّال في مكافحة الجريمة وضبط المجرمين وجمع البيانات والمعلومات المتعلقة بالمجرم والجريمة وتبادلها فيما بينها ، وذلك من خلال المكاتب المركزية الوطنية للشرطة الدولية الموجودة في الدول الأعضاء[2]. كما تسعى مساعدة أجهزة الشرطة في

---

(1) تعد الاتفاقية الدولية الخاصة بمكافحة الرقيق الأبيض لعام 1904م، بداية التعاون الدولي الشرطي، حيث تنص المادة الأولى منها على انه (تتعهد كل الحكومات المتعاقدة بإنشاء أو تعين سلطة لجمع المعلومات الخاصة باستخدام النساء والفتيات لغرض الدعارة في الخارج، ولهذه السلطة الحق في أن تخاطب مباشرة الإدارة المماثلة لها في كل الدول الأطراف المتعاقدة.)، وخلال عام من تاريخ إبرام هذه الاتفاقية أنشأت سبع دول من الدول الموقعة على هذه الاتفاقية أجهزة لتبادل المعلومات والبيانات الخاصة باستخدام النساء والفتيات لغرض الدعارة في الخارج من أجل القضاء على هذه الجريمة في أقاليمها. - **المرجع** : د.حسين بن سعيد بن سيف الغافري - جرائم الحاسب الآلي - ورقة عمل مقدمة من الأمانة العامة لمجلس التعاون الخليجي لاجتماع اللجنة الفنية المتخصصة بدراسة سبل مكافحة الجرائم الإلكترونية " الإنترنت" الأول والذي أنعقد بمقر الأمانة العامة بالرياض خلال الفترة من 4-2004/4/5م- ص6

(2) يختص المكتب المركزي الوطني للشرطة الدولية بتحقيق الاتصال الشرطي بين الدولة التي ينتمي إليها وبين الأمانة العامة للمنظمة الدولية للشرطة الجنائية في ليون - فرنسا والعكس ،تحقيق الاتصال الشرطي بين السلطات المحلية في دولته والمكاتب المركزية الوطنية للشرطة الدولية في الدول الأخرى مثال النشر عن المجرمين الهاربين من دولته إلى الدول الأخرى توجيه وتلقي القبض على المحرمين الهاربين، وإجراء التحريات حول أولئك الهاربين، والقيام بعمليات القبض عليهم ، وإحالتهم إلى السلطات القضائية المختصة. ويتم الاتصال بين الأمانة العامة لمنظمة الانتربول وبين هذه المكاتب من خلال عدة وسائل اتصال منها جهاز X400 حيث يتم من خلال هذا الجهاز ربط الاتصالات بين شبكة المعلومات لهيئة الاتصالات الدولية التليفونية للدولة التي يتبعها المكتب المركزي وبين شبكة الاتصالات الدولية في فرنسا أو بين الدولتين التي يجري الاتصال بين مكتبيها ، ويتطلب تشغيل هذا الجهاز خبرة فنية عالية =

الدول الأطراف ودعمها وتحسين قدراتها باستمرار لمنع الإجرام ومحاربته وتطوير المعارف والمهارات اللازمة لعمل أجهزة الشرطة على الصعيد الدولي بشكل أكثر فاعلية[1]. وبهدف توفير اتصال فعال وآني بين أجهزة الشرطة في مختلف الدول على نحو يمكنها من تبادل المعلومات بشكل آمن وسريع قامت منظمة الإنتربول بوضع منظومة عالمية للاتصالات الشرطية المأمونة لتوفير الاتصال بين موظفي إنفاذ القانون في جميع الدول الأعضاء على نحو يمكن مستخدمي هذه المنظومة من تبادل المعلومات والبيانات الشرطية الهامة فيما بينهم والاطلاع على قواعد بيانات الإنتربول والحصول على خدماته على مدار الساعة.وقد أحدثت منظومة الاتصال تلك تطويرا جذرياً على صعيد عمل أجهزة الشرطة في الدول الأعضاء إذ تمكن المحققون من الوصول إلى أدوات الإنتربول المتطورة ومن الربط بين معلومات قد تبدو غير متصلة فيما بينها، مما ييسر بالتالي التحقيقات في الجرائم، فضلاً عن أن منظومة الاتصال تلك تمكن أجهزة الشرطة وجهات إنفاذ القانون من تقصي البيانات ومقارنتها في ثوان معدودة، وذلك من خلال وصولهم المباشر إلى قواعد البيانات المتعلقة بالمجرمين المشبوهين أو بالأشخاص المطلوبين[2].

وفي رأيي أن هذه المنظومة هي من إحدى المتطلبات الأساسية لمكافحة الجرائم المعلوماتية، التي تتطلب مثل هذا النوع من السرعة في تقفي الأثر وتبادل المعلومات حول الأجهزة مصدر الهجمات الإلكترونية ومستخدميها، بين أجهزة الشرطة في جميع الدول.

وتقوم منظمة الإنتربول بإعداد برنامج لمكافحة الإجرام المعلوماتي يقوم على التدريب والعمليات، ويعمل على مواكبة التهديدات الناشئة عنه، ويهدف هذا

=من الموظف المختص الذي يتولى العمل عليه، كما يتم الاتصال من خلال وسائل الاتصال الأخرى مثل الاتصال التليفوني، الفاكس والتلكس والمكاتبات البريدية والحقائب الدبلوماسية - راجع سراج الدين الروبي - آلية الانتربول في التعاون الدولي الشرطي - الدار المصرية اللبنانية - الطبعة الثانية 2001 - ص165 -181

(1)http://www.interpol.com

(2) النشرة الإعلامية COM/FS/2011-02/GI-03 - الانتربول - http://www.interpol.com

البرنامج إلى[1]:

أ- تعزيز تبادل المعلومات بين البلدان الأعضاء عن طريق الأفرقة العاملة والمؤتمرات الإقليمية؛

ب- توفير دورات تدريبية لوضع معايير مهنية والتقيد بها[2]؛

ج- تنسيق العمليات الدولية ودعمها؛

د- إعداد قائمة عالمية بأسماء ضباط الاتصال ووضعها بتصرف المحققين في مجال الإجرام المعلوماتي على مدار الساعة؛

ه- مساعدة الدول الأعضاء على التحقيق في الهجمات أو الجرائم المعلوماتية عن طريق توفير خدمات في مجال التحقيق وقواعد البيانات؛

و- إقامة شراكات إستراتيجية مع المنظمات الدولية الآخرى وهيئات القطاع الخاص؛

ز- تحديد التهديدات الناشئة وتبادل معلومات الاستخبار في هذا المجال مع الدول الأعضاء؛

ح- توفير بوابة مأمونة على الويب لنشر معلومات ووثائق عملياتية.

وتعمل منظمة الإنتربول حالياً على إنشاء مجمّع عالمي للابتكار في مجال الكشف عن الجرائم في سنغافورة يسمى (مجمع الإنتربول العالمي للابتكار) ليكون مكمّلا لمقر الأمانة العامة للإنتربول في ليون (فرنسا) وذلك بحلول عام 2014، ويوفر هذا المجمّع أكثر الإمكانات تقدما على صعيد البحوث والتطوير

---

(1)http://www.interpol.com

(2) مثال : إعداد تدريب مشترك بين الإنتربول والأوساط الأكاديمية يركز على مكافحة الجريمة الإلكترونية في شهر أغسطس 2011 يشارك فيها محققون في الجريمة السيبرية ومختصون في العلوم الجنائية الحاسوبية من 21 بلدا تُنظّم بمشاركة جامعة دبلن لتدريب على مكافحة الجريمة الإلكترونية. ويهدف هذا البرنامج إلى إنماء المعارف والمهارات النظرية والعملية في عدة مجالات لمساعدة المحققين على التحقيق بفعالية أكبر في الجريمة السيبرية. وهذه المجالات هي التالية: نسخ بيانات القرص الممغنط، التحليل الجنائي لبيانات المباشرة، التحليل الجنائي للهاتف النقال، التحقيق في غسل الأموال،تقنيات التفتيش والضبط،،التحقيقات المتعلقة بالبيانات اللاسلكية وبروتوكول الاتصال الصوتي عبر الإنترنت،الكشف عن الفيروسات وتحليلها. - المرجع: http://www.interpol.int

للكشف عن الجرائم وتحديد هوية المجرمين، ووضع البرامج التدريبية المبتكرة، وتقديم الدعم الميداني، وإقامة الشراكات، وذلك لمواجهة التحديات المتزايدة التي تواجه أجهزة الشرطة في جميع أنحاء العالم تحديات على صعيد العمليات، إذ يستغل المجرمون التكنولوجيا الحديثة وسهولة السفر من بلد إلى آخر وإمكانية عدم الكشف عن هويتهم، التي يُتيحها تنفيذ أعمالهم على الإنترنت.حيث أضحت الظواهر الإجرامية أكثر عدوانية وتعقيدا، وخالصة في مجال الجريمة المعلوماتية. كما يهدف هذا المجمع إلى تجاوز أنشطة النموذج التقليدي للعمل الشرطي المستند إلى رد الفعل. حيث يعمل على توفير مناهج بحث استباقية في مجالات جديدة وأحدث تقنيات التدريب. ويتمثل الغرض من ذلك في تزويد أجهزة الشرطة في جميع أنحاء العالم بالأدوات والقدرات الضرورية لمواجهة التحديات التي تزداد تطورا والتي يطرحها المجرمون بمزيد من البراعة، ومن أهم المكونات الرئيسية للمجمّع العالمي هذا والمتعلق بموضع بحثنا،هو قسم الابتكار والبحوث والأمن الرقمي والذي يهدف إلى:

أ- تعزيز الأمن المعلوماتي ومواجهة الجريمة المعلوماتية.

ب- إنشاء مختبر جنائي لدعم التحقيقات في الجرائم الرقمية.

ج- إجراء بحوث لاختبار البروتوكولات والأدوات والخدمات ولتحليل توجّهات الهجمات المعلوماتية.

د- إيجاد حلول عملية بالتعاون مع أجهزة الشرطة ومختبرات البحث والمجتمع الأكاديمي والقطاعين العام والخاص.

هـ - معالجة مسائل مثل إدارة أمن الإنترنت.[1]

ومن الأمثلة على دور الإنتربول في ما يتعلق بالجرائم المعلوماتية، قيام القضاء اللبناني بتوقيف أحد الطلبة الجامعين في لبنان بتهمة إرسال صور إباحية لقاصرة دون العشرة أعوام من موقعه على شبكة الإنترنت وذلك إثر تلقي النيابة

---

(1) http://www.interpol.int/ar

اللبنانية برقية من الإنتربول في ألمانيا بهذا الشأن[1].

ومن أحدث القضايا في هذا المجال تصريح المسئول في وزارة العدل للكيان الإسرائيلي (يورام هاكوهين) لإذاعة الجيش الإسرائيلي في 8 يناير 2012بأنه يصعب التحقق من هوية «الهاكر» السعودي الذي تمكن من الحصول على المعلومات السرية الخاصة بآلاف الإسرائيليين من حملة بطاقات الائتمان، بما في ذلك عناوين بريدهم الإلكتروني وكلمات السر الخاصة بها، وأن إسرائيل قد تلجأ إلى الشرطة الدولية لملاحقته[2].

ثانيا: جهود شبكة المعلومات التابعة لمجموعة دول الثمانية (مجموعة الدول الصناعية الثمانية)[3] لمواجهة الجرائم المعلوماتية

اعتمد وزراء العدل والشئون الداخلية لدول مجموعة الثمانية خلال اجتماعهم الذي عقد بواشنطن في ديسمبر 1997، المبادئ التي تشكل الأساس لشبكة نقاط اتصال وطنية، تعنى بالجرائم المتصلة بالتكنولوجيا والمساعدة في التحقيق فيها،وتضمنت النشرة الصحفية الختامية للقاء أنه تم التوصل لاتفاق يقضي بتنسيق الخطوات المشتركة من أجل:

- إدخال عدد كاف من المتخصصين القادرين على توفير التعاون التقني في

---

(1) د.حسين بن سعيد بن سيف الغافري- مرجع سابق – ص8

(2) http://saudialyoum.com/NewsDetails.aspx?NewsID=6653، وتخلص قضية هذا الهاكر السعودي والمدعو (x Omar) بأنه في يناير 2012 قام باختراق والحصول على معلومات عن آلاف البطاقات المصرفية الإسرائيلية أكثرمن 20 ألف بطاقة مصرفية ونشرها عقب اختراقه للموقع.ووفقا لموقع "واي نت" الإسرائيلي الذي نشر رداً وصله بالإيميل من شخص قال إنه الهاكر الذي سرق آلاف الوثائق والبطاقات الإسرائيلية، إنه في العاصمة السعودية، ويتحدى الوصول إليه، موضحاً أنه ليس مبتدئاً بل هو على دراية متقدمة بالتقنية، ولن يعثروا عليه مهما أرسل من ملفات وإيميلات، وأنه لا يعتبر إسرائيل إلا فلسطين المحتلة.

وقد ذكرت صحيفة "يديعوت أحرنوت" أن الهاكر الذي يطلق على نفسه "0"x Omar، نشر قائمة تحتوي على العديد من التفاصيل الخاصة بحوالي 11 ألف إسرائيلي، تضمنت أسماءهم وأرقام هواتفهم، والعناوين الدقيقة لأماكن سكناهم، وجميع أرقام بطاقات الائتمان والاعتماد الخاصة بهم، متوعداً بالكشف عن 80 ألف بطاقة مصرفية أخرى، **المرجع**

http://www.alarabiya.net/articles/2012/01/07/186831.html

(3) تضم هذه المجموعة الدول الصناعية الكبرى في العالم وهي :الولايات المتحدة الأمريكية، اليابان، ألمانيا،روسيا الاتحادية، إيطاليا، المملكة المتحدة، فرنسا، وكندا.

مجال مكافحة الجريمة بمجالات التكنولوجيا الرفيعة في صفوف أجهزة قوات حفظ الأمن؛

- وإعداد طرق لمتابعة الهجمات على شبكات الحاسبات الإلكترونية واكتشاف المتسللين خلال أقصروقت؛

- وإجراء تحقيقات في الدول التي يختفي فيها متهمون في حال عدم إمكانية تسليمهم؛

- وإتباع إجراءات كفيلة بالحفاظ على شبكات المعلوماتية والحاسبات الإلكترونية ومنع التطاول عليها؛

- وإعداد طرق جديدة لاكتشاف ومنع جرائم الحاسبات الإلكترونية؛

- واستخدام تكنولوجيا جديدة مثل: خطوط الاتصالات المرئية التي تسمح بالحصول على شهادات شهود من الدول الآخرى[1].

وقد أنشأت هذه الشبكة على غرار الانتربول في الفترة ما بين عامي 1998و 2000،وتضم حاليا في عضويتها ما يزيد على 50 دولة وتشجع الدول على الانضمام إليها، وتميزت هذه الشبكة بقدرتها على الاستجابة لطلبات المساعدة الموجهة إليها على مدار الساعة وفي كل أيام الأسبوع (7/24). وتتميز هذه الشبكة بأنها متخصصة في التحقيقات المتعلقة بالجرائم المعلوماتية، وبقدرتها على استخدام الطرق المناسبة لجمع وحفظ الأدلة الخاصة بتلك الجرائم، وفي يونيو 2001 أصدر مجلس الاتحاد الأوروبي توصية يحث فيها الدول غير الأعضاء في مجموعة الدول الثمانية على الانضمام إلى هذه الشبكة[2]

---

(1) أ.د.محمد البخاري- بحث بعنوان تأثير الانترنيت على تطور المجتمعات - 2010 منشور على الموقع الالكتروني.
http://muhammad-2009.blogspot.com/2010/02/blog-post_27.html

(2) جان فرنسوا هنروت - مرجع سابق - صـ 101 - 102

الفرع الثاني

جهود الأجهزة الإقليمية لمكافحة الجرائم

في مجال مواجهة الجرائم المعلوماتية

تضطلع الأجهزة الإقليمية المتخصصة في مجل مكافحة الجرائم، بدور رئيسي في التصدي لكثير من الجرائم وخاصة الجرائم عبر الوطنية والتي من أبرز تطبيقاتها الجرائم المعلوماتية، وفي هذا الفرع سنتناول دور أهم تلك المنظمات في مجال مواجهة الجرائم المعلوماتية:

أولاً: الشرطة الأوربية (يوروبول – Europol)

على غرار منظمة الانتربول أنشأ الاتحاد الأوربي شرطة أوربية مشتركة تسمى (يوروبول) مكتب الشرطة الأوربية مقرها لاهاي - هولندا ، والاسم باللغة الإنجليزية (Europol) وهو اختصار لـ European Police Office، وذلك بموجب اتفاقية ماستريخت – هولندا عام 1992، والمعروفة رسميا باسم (معاهدة الاتحاد الأوروبي) حيث أنها الاتفاقية المؤسسة للاتحاد الأوروبي. وقد بدأت الشرطة الأوروبية في مباشرة كامل أنشطتها في عام 1999. وقد تم إنشاء اليوروبول ليكون همزة وصل بين أجهزة الشرطة الوطنية في دول الأعضاء ولملاحقة الجناة في الجرائم العابرة للحدود ومنها بطبيعة الحال الجرائم المتعلقة بالإنترنت وذلك من خلال وحدة أو مكتب وطني ينشأ لهذا الغرض في كل دولة من الدول الأعضاء في الاتحاد الأوروبي ، وتقدم هذه الوحدات أو المكاتب بصورة منتظمة المساعدة لليوروبول سواء من تلقاء أنفسهم أو بناء على طلب من مجلس إدارة اليوروبول أو المدير، ويعمل اليوروبول حالياً مع جهات تنفيذ القانون في (27) دولة من أعضاء الاتحاد الأوروبي، بالإضافة إلى الشراكة مع جهات تنفيذ القانون في دول خارج الاتحاد الأوروبي مثل استراليا وكندا والولايات المتحدة والنرويج. وتجدر الإشارة إلى أن ضباط اليوروبول لا يملكون صلاحيات مباشرة لاعتقال المجرمين، وإنما يقومون بدعم جهات

تنفيذ القانون في الدول الأعضاء من خلال جمع وتحليل ونشر المعلومات وتنسيق العمليات بينهم في سبيل منع وكشف الجرائم والتحقيق فيها، وملاحقة ومحاكمة مرتكبيها. كما يقوم اليوروبول بتقديم المساندة والدعم للدول الأعضاء ومساعدتها في حل القضايا الجنائية بشكل سريع من خلال إرساله فرق من الخبراء والمحللين الجنائيين التابعين له للمشاركة في التحقيقات التي تجريها الدولة. ويشرف على اليوروبول مجلس الوزراء لشؤون العدل والداخلية الذي يتألف من وزراء العدل والشؤون الداخلية من جميع الدول الأعضاء في الاتحاد الأوروبي. حيث يقوم هذا المجلس بتوجيه اليوروبول .وتعيين مديره ونواب المدير، كما يختص بإقرار الميزانية الخاصة به، والتي تعد جزءً من الميزانية العامة للاتحاد الأوروبي، كما يختص المجلس أيضاً باعتماد اللوائح المنظمة لعمل اليوروبول، وفي كل عام يقوم المجلس بإعداد تقرير عن عمل اليوروبول ويرفعه.إلى البرلمان الأوروبي. في حين يختص مجلس إدارة اليوروبول بالتوجيه الاستراتيجي والإشراف المباشر على تنفيذ المهام الموكلة إليه. ويتكون هذا المجلس من ممثلين عن الدول الأعضاء والمفوضية الأوروبية ويصدر قراراته بأغلبية الثلثين، يكون لكل عضو صوت واحد. ويجتمع مجلس الإدارة مرتين على الأقل في السنة لمناقشة الموضوعات والقضايا المتعلقة بعمل اليوروبول والتي تتصل بالوضع الحالي له أو بالنسبة للمشروعات المستقبلية. ويقوم مجلس الإدارة كل عام بإعداد ميزانية اليوروبول النهائي، وإعداد برنامج عمله،وإعداد تقرير عام عن الأعمال التي تم تنفيذها خلال العام، ويقوم برفع هذا التقرير إلى مجلس الوزراء لشؤون العدل والداخلية للتصديق عليه تمهيدا لرفعه من قبل الأخير للبرلمان الأوروبي.[1]

ثانياً: وحدة التعاون القضائي الأوروبية (يوروجست - EUROJUST):

وحدة التعاون القضائي الأوروبية، The European Union's Judicial Cooperation Unit وهي هيئة اتحادية، أنشئت بقرار من مجلس الاتحاد

(1) https://www.europol.europa.eu

الأوروبي في عام 2002 ، بهدف تدعيم مكافحة كل الأشكال الخطيرة للإجرام، وتعزيز التعاون القضائي في مجال مكافحة الجريمة، وتسهيل تنسيق عمل التحقيقات والمتابعات القضائية في الدول الأعضاء، بخصوص الجرائم الخطيرة. وقد ولدت فكرة إنشاء وحدة للتعاون القضائي لأول مرة في اجتماع رؤساء دول وحكومات المجلس الأوروبي في تامبيري- فنلندا، في عام 1999، بهدف خلق مساحة من الحرية والأمن والعدالة في الاتحاد الأوروبي، تقوم على التضامن وعلى تعزيز مكافحة الجريمة العابرة للحدود من خلال تعزيز التعاون بين السلطات.وكان لهجمات 11 سبتمبر 2001 في الولايات المتحدة الأمريكية دورٌ كبيرٌ في تسريع إنشاء اليوروجست كوحدة للتنسيق القضائي مع التركيز على مكافحة الإرهاب.

وتتمثل مهام يوروجست تحفيز وتحسين التنسيق بين السلطات المختصة في الدول الأعضاء في التحقيقات والملاحقات القضائية وكذلك تحسين التعاون بين تلك السلطات في مجال تسهيل تنفيذ المساعدة الدولية القانونية المتبادلة وتنفيذ طلبات سليم المجرمين .و يدعم اليوروجست بكل الوسائل الممكنة السلطات المختصة في الدول الأعضاء من أجل إجراء التحقيقات والملاحقات القضائية بالنسبة للجريمة عابرة الحدود.ويشمل اختصاص يوروجست نفس أنواع الجرائم التي تدخل في اختصاص اليوروبول ، مثل الإرهاب وتهريب المخدرات والاتجار بالبشر والتزوير وغسيل الأموال، وجرائم الحاسوب والجرائم ضد الممتلكات أو السلع العامة بما في ذلك الغش والفساد، والجرائم الجنائية التي تؤثر المصالح المالية للجماعة الأوروبية،والإجرام المعلوماتي، والجريمة البيئية والمشاركة في المنظمات الإجرامية .والأنواع الآخرى من الجرائم، ويقدم يوروجست مساعدته في التحقيقات والملاحقات القضائية، بناء على طلب من دولة عضو.ويملك اليوروجست أن يطلب من السلطات المختصة في الدول الأعضاء لاتخاذ إجراء من الإجراءات الآتية:

- التنسيق بين السلطات القضائية في الدول الأعضاء.

- تسهيل العمل في مجال المساعدة القضائية الدولية ، وتنفيذ طلبات تسليم المجرمين.

- الطلب من سلطات الدول الأعضاء تشكيل فرق مشتركة للتحقيق ، عند الحاجة.

- تبادل المعلومات المفيدة مع السلطات المختصة في الدول الأعضاء مع ضمان طابع حماية خصوصيات الأفراد.

- تزويد يوروجست بالمعلومات اللازمة للقيام بمهامه.

وقد أنشئ يوروجست نقاط الاتصال في (24) دوله من خارج الاتحاد الأوروبي ومنها: ألبانيا، الأرجنتين، البوسنة والهرسك، كندا، مصر، جمهورية مقدونيا اليوغوسلافية السابقة، وأيسلندا، وكرواتيا، اليابان، كوريا، ومولدوفا، ومنغوليا، والجبل الأسود والنرويج والاتحاد الروسي وصربيا ، سنغافورة، سويسرا، تايلاند، تركيا، أوكرانيا والولايات المتحدة.[1]

ثالثاً: المكتب العربي للشرطة الجنائية:

على المستوى العربي نجد أن مجلس وزراء الداخلية العرب قد أنشأ المكتب العربي للشرطة الجنائية في عام 1965 بناءً على الاتفاقية الخاصة بإنشاء المنظمة العربية للدفاع الاجتماعي ضد الجريمة، حيث كان مكتب الشرطة الجنائية في دمشق، أحد مكاتبها المتخصصة، ويمارس هذا المكتب نشاطه من خلال ثلاث وزارات (الداخلية، العدل ، الشؤون الاجتماعية) على مستوى الدول العربية [2]

ويختص هذا المكتب بتأمين وتنمية التعاون بين أجهزة الشرطة في الدول الأعضاء في مجال مكافحة الجريمة وملاحقة المجرمين في حدود القوانين

---

(1) http://www.eurojust.europa.eu

(2) موقع جامعة نايف العربية للعلوم الأمنية /http://nauss.edu.sa

والأنظمة المعمول بها في كل دولة. بالإضافة إلى تقديم المعونة التي تطلبها الدول الأعضاء من أجل دعم وتطوير أجهزة الشرطة[1].

ومن جانبي أقترح أن تقوم جامعة الدول العربية بإنشاء شبكة عربية لها نقاط اتصال وطنية في كل دولة عربية متخصصة بالجرائم المتصلة بالتكنولوجيا والمساعدة على التحقيق فيها على شبكة المعلومات التابعة لمجموعة دول الثمانية، تضم المتخصصين القادرين على توفير التعاون التقني في مجال مكافحة الجريمة بمجالات التكنولوجيا الرفيعة في صفوف أجهزة قوات حفظ الأمن، وإعداد طرق لمتابعة الهجمات على شبكات الحاسبات الإلكترونية واكتشاف المتسللين خلال أقصروقت، وإجراء تحقيقات في الدول التي يختفي فيها متهمون في حال عدم إمكانية تسليمهم، وإعداد طرق جديدة لاكتشاف ومنع جرائم الحاسبات الإلكترونية،واستخدام تكنولوجيا التي تسمح بالحصول على شهادات شهود من الدول الآخرى، الأمر الذي يشكل دعماً كبير للدول العربية في مكافحة تلك الجرائم من جهة، وكجهة تنسيق بين الدول العربية بعضهم البعض، وبينهم وبين باقي المنظمات العالمية والإقليمية الآخرى في ذات المجال. فضلا عما لذلك من فائدة إقليمية وعالمية، فزيادة أجهزة مكافحة الجرائم المعلوماتية، هو زيادة في تضيق الخناق على مرتكبيها.

---

(1)موقع المكتب العربي للشرطة الجنائية

http://www.aim-council.org/CriminalPolice/Pages/default.aspx

المطلب الثاني

المساعدة القضائية المتبادلة

تعرف المساعدة القضائية الدولية بأنها " كل إجراء قضائي تقوم به دولة من شأنه تسهيل مهمة المحاكمة في دولة آخري بصدد جريمة من الجرائم"[(1)].

وتتمتع المساعدة القضائية بأهمية كبيرة في مجال مكافحة الجرائم المعلوماتية بشكل عام، والماسة بسرية المعلومات الإلكترونية بشكلٍ خاص حيث أن جرائم الدخول غير القانوني والبقاء غير القانون داخل النظام المعلوماتي والاعتراض غير القانوني للمعلومات الإلكترونية تشكل نموذجا للجرائم المعلوماتية عابرة الحدود حيث أنها في معظم حالتها ترتكب عن بعد وعبر الحدود. وسنتناول في هذا المطلب أهمية المساعدة القضائية المتبادلة ومجالاتها.

الفرع الأول

أهمية المساعدة القضائية المتبادلة

في غالب الأحيان يتعدى أثر الجرائم المعلوماتية حدود الدول، فقد يكون مرتكب الهجوم في بلد ما ويتم شن الهجوم من حواسيب موجودة في بلد آخر، وتقع الآثار المترتبة على ذلك في بلد ثالث، وقد يرتكب المجرم جميع مراحل جريمته في دولة لم تطأها قدماه أصلاً من قبل. لذا تقتضي فعالية التحقيق والملاحقة القضائية تتبع أثر النشاط الإجرامي من خلال تقفي أثر قناة الاتصالات بالحاسبات مصدر الهجوم والحاسوب الضحية أو بأجهزة آخرى تعمل مع مقدمي خدمات الانترنت في دول مختلفة. ولتحديد مصدر الجريمة، غالبا ما يتعين على أجهزة التحقيق الاعتماد على السجلات التاريخية التي تبين متى أجريت توصيلات مختلفة ومن أين، ومن الذي أجراها. وفي أحيان آخرى، قد يتطلب إنفاذ القانون تتبع أثر التوصيل وقت إجرائه، وقد يصطدم المحقوقون أثناء ذلك بصعوبات قانونية تنجم عن مشاكل الحدود والولايات القضائية

---

(1)د.حسين بن سعيد بن سيف الغافري – مرجع سابق – صـ 12

عندما يكون مقدموا الخدمات خارج نطاق الولاية القضائية الإقليمية لهم، وهو ما يحدث في أغلب الأحيان، وهنا تظهر أهمية المساعدة القانونية والقضائية المتبادلة بين سلطات التحقيق في الولايات القضائية في مختلف الدول.

فيما مضى كان التعاون القضائي والقانوني بين الدول محدوداً لعدة أسباب أبرزها تعقيدات وبطء إجراءات تبادل المساعدة القضائية التقليدية وعدم فاعليتها، ، فقد يستغرق اتخاذ الإجراء شهوراً، الأمر الذي لا يتناسب مع ضرورة توخي السرعة في التعامل مع الأدلة الرقمية غير الملموسة وسريعة الزوال.

ومن زاوية آخرى قد يؤدي غياب المساعدة القانونية والقضائية المتبادلة أو بطئها، إلى أن يجري المحققون في إحدى الدول التي تسعى إلى الحصول على المعلومات في حواسيب موجودة في دولة آخرى عمليات بحث عابرة للحدود تكون هي الآخرى غير مرخص بها في النظم الحاسوبية[1].

لذا فأنه لابد من اعتماد آليات للتعاون وتبادل المساعدة تتلاءم مع طبيعة الجرائم المعلوماتية تمكن المحققين في تلك الجرائم من الحصول على المعلومات بصورة عاجلة، ومن الأمثلة العملية التي تبين أهمية التعاون والمساعدة القضائية المتبادلة، قضية معروفة بـ (عملية كاتريك – Catterick Operation) وتتلخص وقائع هذه القضية في قيام إحدى شركات القمار بعملية ابتزاز عبر شبكة الانترنت في الفترة من مايو إلى أكتوبر من عام 2004، وقد نفذ هذه العملية عدد من المجموعات الإجرامية التي تنشط في الإجرام الإلكتروني، وكان أفراد هذه المجموعات يقومون بمراسلة إحدى الشركات لمطالبتها بمبلغ من المال، مهددينها بأنه في حالة امتناعها عن دفع المبلغ المطلوب، فسيقومون بشن هجوم على موقعها الإلكتروني بهدف حجب خدماتها (هجمات حجب الخدمة الموزعة وتسمى أيضا بهجمات الحرمان من الخدمات -DDOS)[2]، ونفذت هذه

---

(1)تدابير لمكافحة الجرائم المتصلة بالحواسيب – ورقة عمل مقدمة في مؤتمر الأمم المتحدة الحادي عشر لمنع الجريمة والعدالة الجنائية، بانكوك 18 – 25 نيسان/ أبريل 2005- ص17

(2) هجمات الحرمان من الخدمات" أو "هجمات حجب الخدمة (DoS) وهي اختصار للعبارة Denial-of-Service وهي تعني حجب أو منع الخدمة وهي هجمات تتم عن طريق إغراق المواقع بسيل من=

المجموعة هجمات حجب الخدمة الموزعة لتثبت للشركات قدرتها على تنفيذ ما تهدد به. وقد نفذت هذه المجموعة الإجرامية هجماتها باستخدام شبكة (البوت نت Botnet) وهي عبارة عن شبكة من أجهزة الكومبيوتر المصابة بفيروس، يتحكم فيها المخترق بتنشيط هذه الأجهزة وإجبارها على زيارة موقع معين في الوقت نفسه، دون أن يدرك أصحابها أنهم يشتركون في هذا العمل الإجرامي.وقد تعرض لهذا الهجوم حوالي (57) شركة في مختلف أنحاء العالم، منها (10) شركات في المملكة المتحدة تجاوزت خسائرها 30 مليون جنيه إسترليني، فضلا عن الضرر الذي تتعرض له المواقع ذاتها حيث أن مقدار البيانات التي يتم توجيهها عبر قسم الوصلات الرئيسية لشبكة الانترنت يكاد يتسبب في تدمير هذه المواقع،وقد تطلب التحقيق في هذه القضية التنسيق بين سلطات التحقيق في كل من الولايات المتحدة الأمريكية والمملكة المتحدة، وقد أسفرت التحريات التي تمت بين أجهزة الشرطة في البلدين إلى وجود أشخاص مشتبه بهم في دولة لاتفيا، فتم تقديم طلب الإنابة القضائية إلى السلطات في لاتفيا، وعليه قام جهاز الشرطة فيها بعملية مراقبة سرية أسفرت عن إلقاء القبض على عشرة أشخاص يشتبه في تورطهم في عمليات غسل أموال.وفي وقت لاحق تم تحديد موقع جهاز كومبيوتر تم اختراقه، وتم أخذ نسخة من الشفرة الخبيثة الموجودة عليه، مما قاد المحققين إلى قناة محادثة عبر الانترنت، وقام رجال الشرطة بمراقبة غرف المحادثة هذه وتوصلوا إلى أن المتحكم في شبكة (البوت نت) المستخدمة في جريمة حجب الخدمة الموزعة، يدخل عادة هذه القناة لشن هجومه، وتم تحديد الأفراد الأعضاء في هذه القنوات[1].

=البيانات غير اللازمة يتم إرسالها عن طريق أجهزة مصابة ببرامج تسمى(*DDOS Attacks*) تعمل على نشر هذا الهجمات بحيث يتحكم فيها القراصنة والعابثين الإلكترونيين لمهاجمة الشبكة (الإنترنت)عن بعد بإرسال تلك البيانات إلى المواقع بشكل كثيف مما يسبب بطء الخدمات أو زحاماً مرورياً بهذه المواقع ويسبب صعوبة وصول المستخدمين لها نظراً لهذا الزحام. المرجع /http://ar.wikipedia.org

(1) أشار إلى هذه القضية راسل تايلر – أهمية التعاون الدولي في منع جرائم الإنترنت - برنامج تعزيز حكم القانون في بعض الدول العربية مشروع تحديث النيابات العامة - بحث مقدم بالندوة الإقليمية حول (الجرائم المتصلة بالكومبيوتر) في الفترة 19-20 نيسان / يونيو 2007 المملكة المغربية- صـ 112-113

وتلخص لنا هذه القضية مدى أهمية وضرورة التعاون وتبادل المساعدة في مجال مكافحة هذه الجرائم المعلوماتية، والذي بات فرضاً لا خياراً بحكم طبيعة تلك الجرائم.

الفرع الثاني

مجالات المساعدة القضائية المتبادلة

تتنوع وتتعدد مجالات المساعدة القضائية المتبادلة في مجال مكافحة الجريمة، ويمكن تقسيمها إلى مجالات عامة تستهدف مختلف الجرائم والتي غالبا ما تتضمنها اتفاقيات عامة مثل معاهدة الأمم المتحدة النموذجية بشأن نقل الإجراءات في المسائل الجنائية ، والاتفاقية الأوروبية لنقل الإجراءات الجنائية ، النموذج الاسترشادي لاتفاقية التعاون القانوني والقضائي الصادر عن مجلس التعاون الخليجي 2003م ،واتفاقية الرياض العربية للتعاون القضائي1983، ومجالات خاصة تتطلبها طبيعة الجريمة المستهدفة مكافحتها، مثل مكافحة الجرائم الإرهاب الدولي، أو الاتجار بالبشر، أو الجرائم المعلوماتية محل بحثنا هذا، وعادة ما ترد هذه المجالات ضمن الاتفاقيات الدولية أو الإقليمية التي أبرمت لغرض مكافحتها، مثل اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية 2000م[1]،اتفاقية بودابست المتعلقة بالجريمة الإلكترونية 2001 والاتفاقية العربية لمكافحة جرائم تقنية المعلومات 2010.

وفي ضوء ما تقدم، سنتناول في هذا الفرع مجالات المساعدة القضائية المتبادلة التقليدية التي يمكن الاعتماد عليها في مجال مكافحة الجرائم المعلوماتية، ونحيل إلى الفرع التالي مجالات المساعدة المتبادلة الخاصة بمواجهة الجرائم المعلوماتية، وذلك على النحو الأتي:

1- نقل الإجراءات:

يقصد بنقل الإجراءات قيام إحدى الدول بناء على اتفاقية أو معاهدة باتخاذ إجراءات جنائية وهي بصدد جريمة ارتكبت في إقليم دولة أخرى ولمصلحة هذه

(1) وقد وافقت عليها مملكة البحرين في عام 2004 بموجب القانون رقم (4) لسنة 2004 بالموافقة على انضمام مملكة البحرين إلى اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية والبروتوكولين المكملين لها

الدولة متى ما توافرت شروط معينة[1] .

ولقد نصت الفقرة الأولى من المادة (1) من معاهدة الأمم المتحدة النموذجية بشأن نقل الإجراءات في المسائل الجنائية 1990م على أنه (إذا اشتبه في أن شخصا ما قد ارتكب عملا يجرمه قانون دولة طرف متعاقد، جاز لتلك الدولة أن تطلب إلى دولة آخرى تكون طرفا متعاقدا اتخاذ القرارات بخصوص هذا الجرم، إذا اقتضت ذلك دواعي إقامة العدل على الوجه السليم.)

ويشترط لنقل الإجراءات ما يأتي[2]:

- التجريم المزدوج ويقصد به أن يكون الفعل المنسوب إلى الشخص يشكل جريمة في الدولة الطالبة والدولة المطلوب نقل الإجراءات إليها.

- شرعية الإجراءات المطلوب اتخاذها بمعنى أن تكون الإجراءات المطلوب اتخاذها مقررة في قانون الدولة المطلوب إليها عن ذات الجريمة.

- أن تكون الإجراءات المطلوب اتخاذها من الأهمية بمكان بحيث تؤدى دورا مهما في الوصول إلى الحقيقة.

- أن لا تكون الجريمة المطلوب نقل الإجراء بشأنها ذو طابع سياسي وفقا لاعتبارات الدولة المطالبة[3].

2- تبادل المعلومات:

ويتم ذلك من خلال تعزيز قنوات الاتصال بين سلطات الدول وأجهزتها ودوائرها المختصة بمكافحة الجرائم ، مثال الأجهزة المختصة بمكافحة جرائم الاتجار والمخدرات، الاتجار بالبشر، الاحتيال، بالإضافة إلى الأجهزة المختصة بمكافحة الجرائم المعلوماتية، ويعتبر إنشاء مثل تلك القنوات ضرورة، وذلك من أجل تيسير تبادل المعلومات بصورة مأمونة وسريعة بشأن كل ما يتعلق

---

(1) د. علي حسن الطوالبة- التعاون القضائي الدولي في مجال مكافحة الجرائم الإلكترونية- ص5- بحث منشور على الموقع الإلكتروني لوزارة الداخلية بمملكة البحرين- /http://www.policemc.gov.bh

(2) د.حسين بن سعيد بن سيف الغافري – مرجع سابق- صـ 13

(3) المادة (7) من من معاهدة الأمم المتحدة النموذجية بشأن نقل الإجراءات في المسائل الجنائية 1990م

بتلك الجرائم، مثل:

1- هوية الأشخاص المشتبه في ضلوعهم في تلك الجرائم وأماكن وجودهم وأنشطتهم، أو أماكن الأشخاص الآخرين المعنيين.

2- حركة عائدات الجرائم أو الممتلكات المتأتية من ارتكاب تلك الجرائم.

3- حركة الممتلكات أو المعدات أو الأدوات الآخرى المستخدمة أو المراد استخدامها في ارتكاب تلك الجرائم.

4- تبادل المعلومات عن الوسائل والأساليب المحددة التي تستخدمها الجماعات الإجرامية المنظمة في ارتكاب جرائمها ، ووسائل وأساليب إخفاء أنشطتها.

5-وتبادل المعلومات وتنسيق التدابير الإدارية وغير الإدارية المتخذة حسب الاقتضاء لغرض الكشف المبكر عن الجرائم .

6-كما يمكن أن تقوم الجهة المختصة في دولة ما بإرسال إلى الجهة المختصة لدى دولة أخرى وهي بصدد النظر في جريمة ما بيانات عن الأحكام القضائية النهائية الصادرة ضد مواطني الأخيرة أو الأشخاص المولودين أو المقيمين في إقليمها والإجراءات التي اتخذت ضدهم والمقيدة في صحف الحالة الجنائية لدى الدولة المرسلة.

وفي تقديري هذا المجال له أهمية كبيرة في مجال مكافحة الجريمة المنظمة وعابرة الحدود بما فيها الجرائم المعلوماتية، وتبرز أهمية هذا المجال من التعاون في ميدان مكافحة الجرائم المعلوماتية التي يلجأ مرتكبيها إلى التحفي على الشبكات الإلكترونية خلف شخصيات وهمية وأسماء مستعارة، وهو ما يتطلب تعاوناً بين الدول خاصة في حالة توزع النشاط الإجرامي بين أكثر من دولة، لتحديد هوية الأشخاص المشتبه في ضلوعهم في تلك الجرائم وتحديد أماكن وجودهم، تمهيداً للقبض عليهم، فضلا عن أن تبادل الدول المعلومات بالنسبة للوسائل

والأساليب التي يستخدمها مرتكبي تلك الجرائم في ارتكاب جرائمها والتي تتسم تلك الوسائل والأساليب بالتطور السريع والمستمر، يسهل من مهمة التصدي لتلك الجرائم، ويجب آن يتم تبادل تلك المعلومات بشكل أكثر سرعة دون انتظار عقد اجتماعات ومؤتمرات لعرض تلك المعومات واستعراض هذه الأساليب، حيث أنه بالإمكان إصدار نشرة دورية شهرية مثلاً تتضمن أحدث الوسائل والأساليب في مجال الجرائم المعلوماتية، على أن يتم تبادلها على مستوى الدول أما بطريق مباشرة (من دولة لدولة) أو من خلال المنظمة الدولية أو الإقليمية والتي بدورها تقوم بتعميمها على الدول الأعضاء بها أو بطرحها على المواقع الإلكترونية الخاصة بها أو عقد الاجتماعات عن بعد بواسطة الشبكات ومناقشة تلك الخبرات. ونقتبس هذه الفكرة من مجرمي المعلومات ذاتهم الذين لا يدخرون جهدا ولا يتوانون عن تبادل خبراتهم في مجال الاختراق والتجسس المعلوماتي سواء من خلال مؤتمراتهم عبر شبكات الانترنت ومن خلال منتدياتهم المخصصة لهذا الغرض.

فعلى سبيل المثال نظم مجموعة من قراصنة الكمبيوتر في أغسطس 2011 مهرجاناً خاصاً بهم في مدينة فونوفورت الألمانية بمشاركة حوالي ثلاثة آلاف و خمسمائة شخص من حوالي خمس وأربعين دولة. ويهدف هذا المهرجان إلى إتاحة الفرصة للمشاركين فيه من قراصنة الكمبيوتر التعرف على آخر الوسائل والأجهزة الإلكترونية الحديثة المستخدمة في هذا المجال وتبادل الخبرات فيما بينهم. وقد ذكرت إحدى المشاركات في هذا المهرجان أن " هذا ليس تجمعاً للمجرمين ولا يحمل نية سيئة، معظم المشاركين هنا جاؤوا للتعرف على أحدث أنواع التكنولوجيا و كيف تعمل، و أين هي حدود التكنولوجيا". وقد تمكن القائمون من تأمين اتصال الانترنت لحوالي خمسة آلاف كمبيوتر تعمل في المهرجان و تحمل في جعبتها كل ما هو جديد في عالم القرصنة[1].

(1) المرجع: http://arabic.euronews.net/2011/08/14/computers-under-canvas-at-hackers-summer-camp

3- **تبادل المعلومات التلقائي:**

قد يتوافر لدى إحدى الدول معلومات هامة، تتعلق بمسائل جنائية تخص دولة أخرى ويمكن أن تحقق تلك المعلومات فائدة للأخيرة أو تساعدها على القيام بالتحريات والإجراءات الجنائية أو إتمامها بنجاح، والتي لا تعلم بوجودها الدولة ذات العلاقة. ففي هذه الحالة، تقوم الدولة التي تحوز تلك المعلومات بالاتصال بالدولة ذات العلاقة والتنسيق معها لتبادل تلك المعلومات دون انتظار تتلقى طلباً بذلك.

إلا أنه في هذه الحالة عادة ما تعطي الاتفاقيات التي تنص على هذه الحالة الحق للدولة الحائزة للمعلومات باشتراط أن تظل المعلومات وخاصة الحساسة أن تظل سرية ولو مؤقتا أو أن تستخدم وفقاً لشروط معينة، حيث إن السرية قد تكون مطلوبة ولازمة في بعض القضايا التي تكون فيها مصالح الدولة مقدمة المعلومات معرضة للخطر من جراء البوح بالمعلومات[1]

بيد أن هذا لا يمنع الدولة الطرف المتلقية من أن تفشي في إجراءاتها معلومات تبرئ شخصا متهما. وفي هذه الحالة، تقوم الدولة المتلقية بإخطار الدولة المحيلة قبل إفشاء تلك المعلومات، وتتشاور مع الدولة الطرف المحيلة إذا ما طلب ذلك. في حالة استثنائية إذا تعذر توجيه إشعار مسبق، قامت الدولة الطرف المتلقية بإبلاغ الدولة الطرف المحيلة بذلك الإفشاء دون إبطاء[2].

4- **التحقيقات المشتركة:**

وهذا النوع من التعاون تفرضه طبيعة الجرائم عابرة الحدود بما فيها الجرائم المعلوماتية، حيث يتطلب التحقيق في تلك الجرائم تشكيل فرق مشتركة بين الجهات المختصة في كل دولة من الدولة التي وقعت بها جزء من الجريمة، مثال على ذلك: شاركت أجهزة الشرطة الخاصة بأربعة دول مجتمعة وهي السويد،

---

(1)د. هلالي عبداللاه أحمد – كيفية المواجهة التشريعية لجرائم المعلوماتية في النظام البحريني على ضوء اتفاقية بودابست – مرجع سابق – ص 260-262

(2)الفقرة (4) من المادة (18) من اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية 2000- ، وقد نصت على هذه الحالة أيضا المادة (26) من اتفاقية بودابست الخاصة بالأجرام الكوني 2001.

والدنمارك، وفنلندا، والنرويج في يونيو 2009، في ضبط مجموعة تطلق على نفسها اسم (محاربي شمال أوروبا الفايكنغ) وهي عبارة عن مجموعة من مجرمي دعارة الأطفال تعمل من خلال الانترنت , وقد تمكنت هذه المجموعة من إيقاع حوالي ثمانين شخصا في شباكها، وكانت تقوم هذه المجموعة بتبادل صور جنسية للأطفال على الانترنت، بالإضافة إلى أنهم كانوا يقومون بتصوير عمليات اعتداء جنسي على ضحاياهم[1].

ومن جانبنا نؤكد على أن التحقيق في الجرائم المعلوماتية وكشف غموضها بشكل أكثر سرعة وفاعلية يتطلب عناصر بشرية مؤهلة علمياً نفياً وتقنياً للتحقيق في مثل تلك الجرائم وتحليل أدلتها وحفظها، وهو ما قد يكون غير متاح لإحدى الدول، مما يشكل عقبة أمامها وقد يترتب عليه إفلات الجناة لو قامت بهذا التحقيق منفردة، مما يجعل من تشكيل فرق تحقيق مشتركة مع دول أكثر تقدما في هذا المجال حلاً لها. وجدير بالذكر أن تشكيل فرق التحقيق هذه لا يقتصر فقط على الدول، وإنما يمكن يتم تشكيل مثل هذه الفرق من أعضاء دولة معينة وأعضاء من المنظمات الدولية أو الإقليمية المتخصصة في مجال مكافحة الجريمة بشكل عام والجرائم المعلوماتية بوجه خاص،مثل الإنتربول واليوروبول والمكتب العربي للشرطة الجنائية، اليوروجست ، وغيرها من المنظمات السالف بيانها، حيث أن دعم ومساندة الدول في مجالات مكافحة الجرائم المعلومات والجريمة بشكل عام والتحقيق فيها وكشفها وملاحقة مرتكبيها، يشكل جزءً هاماً من مهامها الرئيسة. وبطبيعة الحال يتم هذا النوع من التعاون في حدود الاحترام التام لسيادة الدولة الطرف التي سيجري التحقيق داخل إقليمها.

5- الإنابة القضائية:

تعرف الإنابة القضائية بأنها طلب اتخاذ إجراء قضائي من إجراءات الدعوى الجنائية تتقدم به الدولة الطالبة إلى الدولة المطلوب إليها ، لضرورة ذلك في

---

(1) المرجع:

http://arabic.euronews.net/2009/06/16/child-porn-ring-smashed-in-raids/

الفصل في مسألة معروضة على السلطة القضائية في الدولة الطالبة ويتعذر عليها القيام به بنفسها [1].

وقد عرفت المادة (3) من القانون العربي الاسترشادي للتعاون القضائي الدولي في المسائل الجنائية الإنابة القضائية بأنها (قيام الجهة الطالبة بتفويض الجهة القضائية المختصة في الجهة المطلوب إليها لاتخاذ إجراء أو أكثر من إجراءات التحقيق أو من إجراءات تتعلق بالجريمة المطلوب التعاون بشأنها)

وتهدف هذه الصورة إلى تسهيل الإجراءات الجنائية بين الدول بما يكفل إجراء التحقيقات اللازمة لتقديم المتهمين للمحاكمة والتغلب على عقبة السيادة الإقليمية التي تمنع الدولة الأجنبية من ممارسة بعض الأعمال القضائية داخل أقاليم الدول الآخرى .

وقد نصت المادة (14) من اتفاقية الرياض العربية للتعاون القضائي1983[2] على أنه (لكل طرف متعاقد أن يطلب إلى أي طرف متعاقد آخر أن يقوم في إقليمه نيابة عنه بأي إجراء قضائي متعلق بدعوى قائمة وبصفة خاصة سماع شهادة الشهود وتلقي تقارير الخبراء ومناقشتهم، وإجراء المعاينة وطلب تحليف اليمين.)

وعادة وكما هو معهود يتم إرسال طلب الإنابة القضائية عبر القنوات الدبلوماسية [3]، فمثلا طلب الحصول على دليل إثبات في جريمة ما، وهو عادة من اختصاص النيابة العامة تقوم بتوثيقه المحكمة الوطنية المختصة في الدولة الطالبة ثم يمرر بعد ذلك عن طريق وزارة الخارجية إلى سفارة الدولة متلقية

---

(1) د. جميل عبد الباقي الصغير ، الجوانب الإجرائية للجرائم المتعلقة بالإنترنت، دار النهضة العربية، القاهرة 1998م – ص83

(2) وافق على هذه الاتفاقية مجلس وزراء العدل العرب بموجب قراره رقم (1) المؤرخ 1983/4/6 في دورة انعقاده العادي الأولى، في" الرياض" ودخلت الاتفاقية حيز النفاد ابتداء من تاريخ 1985/10/30، وقد صادقت مملكة البحرين على هذه الاتفاقية بموجب المرسوم بقانون رقم (41) لسنة 1999بالتصديق على اتفاقية الرياض العربية للتعاون القضائي لعام 1983.

(3) أنظر مثلا المادة (16) من اتفاقية الرياض العربية لتعاون القضائي1983، والمادة (2) من معاهدة الأمم المتحدة النموذجية بشأن نقل الإجراءات في المسائل الجنائية1990 والمادة (7) من النموذج الاسترشادي لاتفاقية التعاون القانوني والقضائي الصادر عن مجلس التعاون الخليجي 2003م،

الطلب لتقوم هذه الأخيرة بإرساله بعد ذلك إلى السلطات القضائية المختصة في الدولة متلقية الطلب . وما أن يتم تلبية الطلب ينعكس الاتجاه الوارد في سلسلة العمليات[1].

ولقد بينت المادة (426) من قانون الإجراءات الجنائية البحريني لعام 2002 الإجراءات الخاصة بطلب الإنابة القضائية[2]، وهي أن يرسل طلب الإنابة من السلطة المختصة في الدولة الطالبة بالطرق الدبلوماسية ويحال الطلب إلى المحكمة الكبرى الجنائية. وأن يرفق بطلب الإنابة صورة رسمية من أوراق التحقيق الخاصة بالجريمة وبيان واف عن ظروفها وأدلة الاتهام فيها والنصوص القانونية المنطبقة عليها مع تحديد للإجراءات المطلوب اتخاذها والتحقيقات المراد القيام بها. إلا أنه ورغبة في تسريع إجراءات طلب الإنابة القضائية وخاصة في الحالات التي تتطلب اتخاذ إجراء عاجل، فقد أجازت ذات المادة أن تحصل الإنابة عن طريق الاتصال المباشر بين السلطات القضائية المختصة في الدولتين حتى يرد طلب الإنابة بالطرق الدبلوماسية، ولم تحدد المادة نوع الاتصال المباشر وعليه فأنه يمكن أن يشمل طرق الاتصال السريعة مثل الطلب الشفوي عن طريق الاتصال الشفوي أو الفاكس أو التلكس، أو حتى عن طريق البريد الاليكتروني ، وهذا الإجراء منصوص عليه أيضا الفقرة (14) من المادة (18) من اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية 2000. وهذا الاستثناء يتناسب وطبيعة طلبات المساعدة القضائية بشكل عام ذات العلاقة بالجرائم المعلوماتية والتي يجب أن تتسم بالسرعة حتى تتحقق

---

(1) د.حسين بن سعيد بن سيف الغافري- مرجع سابق – ص14

(2) تنص المادة (426) من قانون الإجراءات الجنائية البحريني لعام 2002 على انه (إذا رغبت إحدى الدول الأجنبية في إجراء تحقيق بمعرفة السلطات القضائية بمملكة البحرين يرسل طلب الإنابة من السلطة المختصة في تلك الدولة بالطرق الدبلوماسية ويحال الطلب إلى المحكمة الكبرى الجنائية. ويجب أن يرفق بطلب الإنابة صورة رسمية من أوراق التحقيق الخاصة بالجريمة وبيان واف عن ظروفها وأدلة الاتهام فيها والنصوص القانونية المنطبقة عليها مع تحديد للإجراءات المطلوب اتخاذها والتحقيقات المراد القيام بها.

ويجوز مع ذلك في حالة الاستعجال أن تحصل الإنابة عن طريق الاتصال المباشر بين السلطات القضائية المختصة في الدولتين وذلك حتى يرد طلب الإنابة بالطرق الدبلوماسية.)

الهدف المنشودة منها.

وسعيا وراء الحد من الروتين والتعقيد والبطء التي تتميز بها الإجراءات الدبلوماسية يحدث وبدرجة متزايدة أن تشترط المعاهدات والاتفاقيات الخاصة بتبادل المساعدة القضائية الدولية على الدول الأطراف أن تعين سلطة مركزية – عادة ما تكون وزارة العدل- ترسل إليها الطلبات مباشرة بدلا من الولوج إلى القنوات الدبلوماسية والتي من شأنه تسريع الإجراءات التي قد تأخذ وقتا طويلا فيما لو تم عبر تلك القنوات[1].

---

(1) مثال:المادة الثانية من معاهدة الأمم المتحدة النموذجية بشأن نقل الإجراءات في المسائل الجنائية 1990م.

البند الأول من المادة 30من معاهدة منظمة المؤتمر الإسلامي لمكافحة الإرهاب الدولي 1999م.

المادة 9 من النموذج الاسترشادي لاتفاقية التعاون القانوني والقضائي الصادر عن مجلس التعاون الخليجي 2003م.

الفرع الثالث

مجالات المساعدة المتبادلة الخاصة بمواجهة الجرائم المعلوماتية

لا يزال العديد من الإجراءات الرسمية الواردة باتفاقات المساعدة القانونية المتبادلة القائمة يتسم بنوع من التعقيد والبطء، والذي لا يتناسب مع الطبيعة السريعة للجرائم المعلوماتية. لذا فأنه كان من اللازم استحداث وسائل آخرى للتعاون أكثر سعة وفاعلية للتصدي للجرائم المعلوماتية، وسنستعرض تلك المجالات في ضوء الاتفاقيات الخاصة بالجرائم المعلوماتية مثل اتفاقية بودابست المتعلقة بالجريمة الإلكترونية 2001[1] والاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010.

تنص المادة (23) من اتفاقية بودابست المتعلقة بالجريمة الإلكترونية على أنه (يجب على الأطراف أن تتعاون، مع بعضها البعض وفقاً لأحكام هذا الفصل، في تطبيق الأصول الدولية المتصلة بالتعاون الدولي في المواد الجنائية، والاتفاقيات المعتمدة على التشريعات المتماثلة أو النظيرة والقوانين المحلية،إلى أوسع نطاق ممكن لأغراض التنقيب والتحري أو الإجراءات الجنائية المتعلقة بالجرائم الجنائية المرتبطة بنظم وبيانات معلوماتية أو لجمع أدلة ذات شكل إلكتروني للجريمة الجنائية.).

وقد بينت المادة المذكرة التفسيرية لهذه الاتفاقية أن المادة (23) قد أقرت ثلاث مبادئ عامة تحكم التعاون الدولي وهي كالآتي:[2]

---

(1)تعد اتفاقية بودابست 2001 المتعلقة بالجريمة الإلكترونية نموذجاً عالمياً للاتفاقيات في مجال مكافحة الجرائم المعلوماتية، حيث إن هذه الاتفاقية غير قاصرة على دول الاتحاد الأوروبي، حيث قامت كل من كندا واليابان وجنوب أفريقيا والولايات المتحدة الأمريكية = بالانضمام إليها، كما أنه يمكن لأية دولة في العالم الانضمام لها أيضاً. وتعد هذه الاتفاقية من أول الاتفاقية دولية تعرف جرائم الإنترنت وتتضمن احكام إجرامية محدد وأحكاما تتعلق بالتعاون الدولي . - المرجع كريستينا سكولمان - عن جرائم الإنترنت (طبيعتها وخصائصها- برنامج تعزيز حكم القانون في بعض الدول العربية مشروع تحديث النيابات العامة - بحث مقدم بالندوة الإقليمية حول (الجرائم المتصلة بالكومبيوتر) في الفترة 19-20 نيسان / يونيو 2007 المملكة المغربية- صـ 40

(2)د. هلالي عبداللاه أحمد – كيفية المواجهة التشريعية لجرائم المعلوماتية في النظام البحريني على ضوء اتفاقية بودابست – مرجع سابق – صـ 241- 243

أ) يجب على جميع الأطراف التعاون مع بعضها البعض في أوسع نطاق ممكن، وهذا المبدأ يفرض التزاماً على الدول الأطراف بأن تتعاون مع بعضها على نطاق واسع وأن يزيلوا ما استطاعوا العقبات التي تحول وهذا التعاون في جمع الأدلة وتدفق المعلومات على المستوى الدولي.

والالتزام هنا في تقديري هو التزام بتحقيق نتيجة وليس فقط ببذل عناية، وإلا لن يُؤتي هذا المبدأ ثماره.

ب) إن التعاون لابد أن ينفذ معاً وفقاً لأحكام هذا الفصل الخاص بمواجهة جرائم المعلوماتية عن طريق التعاون الدولي من هذه الاتفاقية ، وتطبيقاً للأصول الدولية المتصلة بالتعاون الدولي في المواد الجنائية والاتفاقيات المعتمدة على التشريعات المماثلة أو النظيرة والقانون المحلي، وبمقتضى هذا المبدأ أن المادة (23) لا تبطل شروط الوثائق الدولية المتعلقة بالمساعدة القضائية وتسليم المجرمين والاتفاقيات الأخرى النظيرة بين الدول الأطراف بالنسبة لهذه الوثائق، أو شروط القانون المحلي المتعلقة بالتعاون الدولي.

وبالإضافة إلى مجالات التعاون الدولية التي تضمنتها اتفاقية التعاون القضائي الدولية والإقليمية على النحو السالف بيانه، فقد تضمنت هذه الاتفاقية بعض صور مجالات التعاون القضائي والتي تتناسب مع طبيعة الجرائم المعلوماتية، وهي كالآتي:

1- المساعدة القضائية المتبادلة في مجال الإجراءات الوقتية والعاجلة؛ وتشمل المجالات الآتية:

أ- **التحفظ العاجل على بيانات الحاسب المخزنة:**

وتناولت هذا الإجراء المادة (29)[1] من هذه الاتفاقية والتي تنص على أنه (1- يجوز لأي طرف أن يطالب طرف آخر أن يأمر أو بالأحرى يتحفظ

---

(1) يقابل هذه المادة، المادة السابعة والثلاثون من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010

على بيانات مخزنة، بواسطة نظام كومبيوتر، يقع داخل إقليم ذلك الطرف الآخر والتي بشأنها ينوي الطرف الطالب تقديم طلب بالمساعدة المتبادلة من أجل البحث أو الدخول على أو مصادرة أو تامين أو كشف هذه البيانات... 3- عند استلام الطلب من الطرف الآخر، يقوم الطرف المطلوب منه، باتخاذ كافة الإجراءات الملائمة وذلك لسرعة التحفظ على البيانات المحددة وفقاً للقانون الوطني. لأغراض الاستجابة، لا يلزم وجود ازدواجية في الجريمة كشرط لتوفير مثل هذا التحفظ. 4- يجوز لأي طرف يشترط وجود ازدواجية في الجريمة كشرط للاستجابة لطلب المساعدة المتبادلة من أجل البحث في بيانات الكومبيوتر، أو الدخول عليها، أو مصادرتها أو تأمينها أو الكشف عنها، بالنسبة للجرائم خلاف تلك المنصوص عليها وفقاً للمواد من 2- 11 من هذه الاتفاقية، أن يحتفظ بالحق في رفض طلب التحفظ بموجب هذه المادة في الحالات التي يتوافر لديه فيها أسباب تدعوه للاعتقاد بأنه في وقت عملية الكشف أو الإفصاح عن هذه المعلومات بتعذر استيفاء الشرط الخاص بوجود ازدواجية في الجريمة)

والمساعدة المتبادلة في التحفظ العاجل على البيانات المخزنة في النظام المعلوماتي المنصوص عليه في المادة السابقة، هو أمر ضروري تستلزمه طبيعة الأدلة في الجرائم المعلوماتية، وذلك لتفادي أي تغيير في هذه الأدلة أو نقلها أو إتلافها ومحو آثار الجريمة، خلال المدة التي تستغرقها إجراءات طلب المساعدة المتبادلة للحصول على تلك البيانات بالطرق التقليدية. وعملية التحفظ هي أجراء ذو طبيعة وقتية للتدخل بطريقة أكثر سرعة من مجرد تنفيذ التماس أو طلب المساعدة المتبادلة التقليدية. بالإضافة إلى ما يتميز به هذا الإجراء من سرعة، فأنه يعد اقل تدخلا حيث إن هذا الإجراء لا يتطلب من سلطات الدولة الموجه إليها طلب المساعدة نزع البيانات من الجهة القائمة عليها والاستحواذ عليها، وإنما مضمون هذا الإجراء أن تقوم تلك السلطات باتخاذ الإجراءات التي تضمن أن الجهة التي بحوزتها المعلومات

موضوع طلب المساعدة والتي غالباً ما تكون هذه الجهة هي مزود الخدمة أو شخص ثالث، لا تقوم بمحو هذه البيانات لحين صدور أمرٌ بتحويلها إلى سلطات إنفاذ القانون في وقت لاحق.

كما يتسم هذا الإجراء بأنه ليس فيه مساس بسرية المعلومات والبيانات محل الإجراء الوقتي موضوع الطلب، فلا يتم كشفها ولا فحصها من قبل سلطات إنفاذ القانون إلا في بعض الحالات ووفقاً للشروط المقررة قانوناً بما يكفل حق الشخص المعني بالمعلومات في الخصوصية بسرية.

ويلاحظ أن البند الثالث من المادة السابقة لم يستلزم كشرط مسبق لتبادل المساعدة في هذا المجال تحقق مبدأ التجريم المزدوج بمعنى أن يكون الفعل المراد تبادل المساعدة بشأنه يشكل جريمة في النظام القانوني للدولتين، وذلك لأن تطبيق هذا الشرط لن يكون منتجاً في مواد التحفظ، وجدير بالذكر أنه يوجد اتجاه نحو استبعاد تطبيق قاعدة التجريم المزدوج بالنسبة لكل الوسائل الإجرائية ما عدا الأكثر تطفلاً أو تدخلاً في الحياة الخاصة كالتفتيش والتنصت، والتحفظ على البيانات والمعلومات المخزنة إلكترونيا لا يعد من وجهة نظر واضعي الاتفاقية من قبيل التطفل أو التدخل في الحياة الخاصة، حيث إن كل ما يفعله الحارس على البيانات أو القائم عليها هو المحافظة على تلك البيانات بأن تبقى في حيازته بشكل قانوني وأن يحافظ عليها من المحو أو الإتلاف، وأن لا يتم الكشف عنها أو فحصها من قبل سلطات الدولة مقدمة الطلب إلا بعد تقديم طلب المساعدة وفقا للإجراءات الرسمية بهدف الكشف عن سرية هذه البيانات والمعلومات.وقد أعطى البند الرابع الدول الأطراف الحق في اشتراط أو التمسك بمبدأ التجريم المزدوج استثناء للرد على طلب المساعدة المتبادلة في هذا المجال، إلا أن نطاق هذا الاستثناء مقيد بالجرائم غير الواردة في المواد 2-11 من هذه الاتفاقية، وهذه الجرائم هي الولوج غير القانوني، والاعتراض غير القانوني، والاعتداء على سلامة البيانات، والاعتداء على سلامة النظام وإساءة استخدام أجهزة الحاسب ومعداته، والتزوير المعلومات، والغش المعلوماتي،

والجرائم المتصلة بالمواد الإباحية، والجرائم المتصلة بالمواد الإباحية الطفولية، الجرائم الواقعة على الملكية الفكرية والحقوق المجاورة، والشروع والاشتراك، بالإضافة إلى تجميع الأدلة تحت شكل الكتروني للجريمة الجنائية. أي أن هذا الاستثناء يمكن أن يطبق بالنسبة للحالات التي تكون فيها الجريمة مرتكبة باستخدام نظام معلوماتي أو بالنسبة للجرائم التي تكون فيها الجريمة لم ترتكب بواسطة نظام معلوماتي ولكن يمكن أن تكون محلاً لجمع أدلة ذات شكل الكتروني.فالجرائم الواردة بالمواد 2-11 يفترض أن شرط التجريم المزدوج قد تم استيفاؤه بطريقة آلية بين الطرفين.[1]

ب- **الإفشاء العاجل لسرية بيانات المرور المتحفظ عليها.**

يتكامل هذا المجال من التعاون مع المجال السابق، ففي غالب الأمر يظهر هذا المجال بمناسبة المجال السابق. فالمادة (30)[2] من ذات الاتفاقية تنص على أنه (1- في حالة إذا ما اكتشف الطرف المطلوب منه، أثناء تنفيذ الطلب المقدم إليه وفقاً للمادة (29) من أجل التحفظ على خط سير بيانات تتعلق باتصال محدد، أن أحد مقدمي الخدمة في دولة آخرى مشتركاً في نقل الاتصال يقوم الطرف المطلوب منه على الفور بالكشف عن القدر الكافي من خط سير البيانات للتعرف على مقدم الخدمة هذا والمسار الذي سلكه الاتصال.)

ما يحدث في هذه الحالة أنه عندما يقوم الطرف المقدم إليه الطلب بتنفيذ ما طلب منه بالتحفظ على بيانات المرور المتعلقة بنقل الاتصال بواسطة مزودي الخدمة بفرض من خلال تتبع مصدر الاتصال لتحديد هوية مرتكب الجريمة أو تجميع الأدلة على ذلك، أنه قد يكتشف أثناء ذلك أن بيانات المرور التي وجدت في إقليمه تشير إلى أن الاتصال قد تم إرساله من خلال مزود خدمات موجود في إقليم دولة ثالثة أو حتى في إقليم الدولة مقدمة الطلب، فأنه في هذه الحالة يجب على الدولة المقدم إليها الطلب أن بالكشف للدولة الطالبة عن القدر الكافي

---

(1) المرجع نفسه- ص276- 277

(2) يقابل هذه المادة، المادة الثامنة والثلاثون من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010

من البيانات من خط سير البيانات الذي يمكنه من التعرف على مزود الخدمة هذا، والمسار الذي سلكه الاتصال. وفي ذلك فائدة للدولة مقدمة الطلب حيث تتمكن من خلال هذه المساعدة معرفة الدولة التي تقدم إليها طلب المساعدة العاجلة بشأن التحفظ على البيانات والمعلومات المخزنة في النظام المعلوماتي، وهكذا حتى يتم الوصول إلى المصدر الحقيقي للاتصال.[1]

وفي رأيي فإن النص السابق يعالج مسألة واقعية هامة تحدث غالبا في أرض الواقع، حيث أنه عادة ما يقوم المجرم المعلوماتي بمحاولة بتوزيع نشاطه الإجرامي عبر أكثر من دولة بقصد تعقيد مهمة البحث عنه وكشف هويته.

2- المساعدة القضائية المتبادلة في مجال سلطات التحقيق: وتشمل المجالات الآتية:

أ- المساعدة المتبادلة الخاصة بالولوج إلى البيانات المعلوماتية المخزنة:

تنص المادة (31)[2] من الاتفاقية على أنه (1- يجوز لأي طرف أن يطلب من طرف آخر القيام بالبحث في بيانات الكومبيوتر، أو الدخول عليها، أو مصادرتها، أو تأمينها أو الكشف عنها، تكون مخزنة بواسطة نظام كومبيوتر داخل إقليم الطرف المطلوب منه، بما في ذلك البيانات التي تم التحفظ عليها وفقا للمادة (29). 2- يستجيب الطرف المطلوب منه الطلب من خلال تطبيق الوثائق والترتيبات والقوانين الدولية المشار إليها بالمادة (23)، وطبقا للنصوص القانونية الأخرى ذات الصلة في هذا الباب...). وتتشابه هذه المادة مع البند (ج) من الفقرة الثانية من المادة (18) من اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية والخاصة بتقديم المساعدة القانونية المتبادلة بالكامل بمقتضى قوانين الدولة متلقية الطلب ومعاهداتها واتفاقاتها وترتيباتها ذات الصلة، بشأن تنفيذ عمليات التفتيش والضبط والتجميد،

---

(1) د. هلالي عبداللاه أحمد – كيفية المواجهة التشريعية لجرائم المعلوماتية في النظام البحريني على ضوء اتفاقية بودابست – مرجع سابق – ص 278- 280

(2) يقابل هذه المادة، المادة التاسعة والثلاثون من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010

وبمقتضى المادة (31) السابقة يحق لإحدى الدول الأطراف في الاتفاقية بمناسبة تحقيقات تجريها في جريمة ما أن تطلب من دولة طرف آخرى يقع على إقليمها النظام المعلوماتي تفتيش هذا النظام والدخول إليه والتحفظ أو مصادرة البيانات المخزنة بداخله لمصلحة الدولة مقدمة الطلب، تماماً كما هو الحال بالنسبة لعمليات التفتيش والضبط التي تجريها الدولة المقدم إليها الطلب على البيانات والمعلومات المخزنة إليكترونياً في النظم المعلوماتية الموجود في إقليمها، وهو ما يفرض على الدول الأطراف أن تكون مؤهلة لتلبية تلك الطلبات من الناحية الفنية والتقنية،ووفقا للبند (2) من هذه المادة فإن يسري بشأن هذا الطلب الشروط المقررة في المعاهدات والاتفاقيات والتشريعات الوطنية المطبقة في هذا الخصوص.

ب- الدخول عبر الحدود إلى البيانات المعلوماتية المخزنة بتصريح أو من خلال إتاحتها للجمهور:

يعد هذا المجال والذي تضمنته المادة (32)[(1)] من اتفاقية بودابست المتعلقة بالجريمة الإلكترونية 2001، من مجالات المساعدة القضائية المتبادلة أفرزته طبيعة الجرائم المعلوماتيا، حيث تنص تلك المادة على أنه (يجوز لأي طرف، وبدون تفويض من أي طرف آخر : أ- الدخول على بيانات كومبيوتر مُخزنة متاحة علناً (مصدر مفتوح)، وبغض النظر عن مكان تواجد البيانات جغرافياً، أو

ب-الدخول على، أو تلقي عن طريق نظام كومبيوتر في إقليمه، بيانات كومبيوتر مُخزنة موجودة في طرف آخر، وذلك في حالة حصول ذلك الطرف على الموافقة القانونية والطوعية من الشخص الذي له السلطة القانونية في الكشف عن البيانات لذلك الطرف من خلال، نظام الكومبيوتر المذكور.)

لقد ثار بشأن المادة السابقة نقاش مطول بين واضعي هذه الاتفاقية قبل إقراره بحالته هذه، حيث كان موضوع النقاش هو متى يكون مسموحاً لأي

---

(1) يقابل هذه المادة، المادة الأربعون من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010

دولة أن تدخل بشكل منفرد إلى بيانات ومعلومات مخزنة على إقليم دولة آخرى، ولقد توصلوا من خلال مناقشتهم لعدة حلول مختلفة إلى تحديد الحالات التي يمكن أن يقبل فيها الدخول بشكل فردي، وتلك التي لا يجوز أن تكون مقبولة، وفي نهاية المطاف خلص أطرف النقاش إلى أن الحلول التي اتفق عليها الجميع هي بشأن الدخول بشكل فردي هي ما يجب أن تتضمنها المادة (32). وقد تضمنت هذه المادة حالتين؛ الأولى عندما تكون المعلومات والبيانات التي تم الوصول إليها متاحة للجمهور أصلا. والثانية عندما يتم الوصول إلى هذه البيانات المخزنة خارج النطاق الإقليمي لدولة طرف أو تلقيها من خلال نظام معلوماتي يقع على إقليمه، وذلك بناء على موافقة قانونية أو إرادية من شخص يملك سلطة قانونية للكشف عنها.[1]

ويمكن تعريف الشخص الذي يملك سلطة قانونية للكشف عن البيانات والمعلومات الإلكترونية بأنه كل شخص طبيعي أو معنوي له كافة السلطات الممكنة بموجب قانون أو اتفاق على البيانات والمعلومات المخزنة إلكترونيا بحيث يحق له استعماله واستغلاله والتصرف فيه،

فقد يحدث في الواقع أن تكون المعلومات المراد الاطلاع عليها بمناسبة التحقيق في جريمة معلوماتية مخزنة في نظام معلوماتي يقع خارج إقليم الدولة التي تجري التحقيق، ففي مثل هذه الحالة يكون بمقدور هؤلاء الأشخاص استعادة البيانات شريطة أن يكون لديهم سلطة قانونية تخولهم ذلك، بالإضافة إلى السلطة بالكشف عنها وذلك بمحض إرادتهم لسلطات إنفاذ القانون، أو أن يسمحوا لهذه السلطات بالدخول إلى هذه البيانات.

ومن جانبي، يستحسن من باب احترام سيادة الدول والمجاملات الدولية ولتفادي أي إشكالية قد تثور بين الدول الأطراف بشأن تفتيش نظام معلوماتي يقع على إقليم إحداهما، أن يتم إضافة شرط بالنسبة للحالة التي تقوم فيها

---

(1) د. هلالي عبداللاه أحمد - كيفية المواجهة التشريعية لجرائم المعلوماتية في النظام البحريني على ضوء اتفاقية بودابست - مرجع سابق - صـ 288- 290

سلطات الدولة بالدخول إلى النظام المعلوماتي الموجود في إقليم الدولة آخرى وتفتيشه و ضبط ما بداخله من معلومات، مفاد هذا الشرط إخطار وإحاطة الدولة التي يقع في إقليمها النظام المعلوماتي المراد تفتيشه علماً، بعملية الدخول وموافقة صاحب السلطة القانونية على تلك المعلومات والبيانات على ذلك.

ج- المساعدة المتبادلة في بخصوص جمع بيانات المرور في الوقت الفعلي:

بداية يقصد ببيانات المرور أو خط سير البيانات وفقاً لأحكام المادة (1) من اتفاقية بودابست الخاصة بالإجرام الكوني 2001 (أي بيانات كومبيوتر متعلقة باتصال عن طريق منظومة كومبيوتر والتي تنشأ عن منظومة كومبيوتر تشكل جزءاً في سلسلة الاتصالات، توضح مصدر الاتصال، والوجهة المرسلة إليها، والطريق الذي تسلكه، ووقت وتاريخ، وحجم، ومدة، ونوع الخدمة المذكورة.) في كثير من الأحيان قد لا يكون بإمكان سلطات التحقيق ضمان تتبع خط سير الاتصال للوصول غلى مصدر الاتصال لإتباع أثره من خلال التسجيلات الخاصة برسائل سابقة، وذلك نتيجة قيام مزود الخدمة بحذف بيانات المرور بشكل آلي من حلقات الاتصال التي تمر بها علمية نقل الرسالة، لذا فأنه من الضروري بالنسبة لسلطات التحقيق في فيكل دولة أن يكون لديها القدرة على الحصول على بيانات المرور خلال الوقت الفعلي بالنسبة للاتصالات التي تمر من خلال نظام معلوماتي لدى دولة آخرى.

لذا فقد نصت المادة (33)[1] من اتفاقية بودابست 2001 على أنه (1- يقدم الأطراف المساعدة المتبادلة لبعضهم البعض فيما يتعلق بتجميع خط سير البيانات بصورة عاجلة، والتي تكون لها علاقة باتصالات محددة في إقليمهم يتم نقلها بواسطة نظام كومبيوتر ، وطبقاً لنصوص الفقرة (2) فإن هذه المساعدات تحكمها الشروط والإجراءات المنصوص عليها في القانون الوطني. 2- يقوم كل طرف بتقديم مثل هذه المساعدة على الأقل فيما يتعلق بالجرائم الجنائية التي

---

(1) يقابل هذه المادة، المادة الحادية والأربعون من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010

يكون فيها تجميع خط سير البيانات بصورة عاجلة متاحاً في قضية محلية مماثلة)

إذا بموجب النص السابق يكون كل طرف ملزماً بتجميع خط سير البيانات بصورة عاجلة وفي الوقت الفعلي لمصلحة الطرف الآخر. ولما كان تجميع بيانات المرور بصورة عاجلة وفي الوقت الفعلي قد يكون الطريقة الوحيدة الجوهرية لتحديد هوية مرتكب الجريمة المعلوماتية، وحيث أن هذا الإجراء أقل تطفلا أو تدخلا ، فإن الفقرة (2) من الاتفاقية قد استخدمت مصطلح (على الأقل) لجميع الدول الأطراف على السماح بأوسع نطاق ممكن للمساعدة المتبادلة بهذا الشأن حتى في ظل غياب مبدأ التجريم المزدوج.

د- المساعدة المتبادلة في مسألة اعتراض بيانات المحتوى :

نصت المادة (34) من ذات الاتفاقية على أنه (يقدم الأطراف المساعدة المتبادلة لبعضهم البعض فيما يتعلق بتجميع أو تسجيل محتوى البيانات بصورة عاجلة والتي تتعلق باتصالات محددة يتم نقلها بواسطة نظام كومبيوتر وذلك بالحد الذي تجيزه الاتفاقيات والقوانين الوطنية واجبة التطبيق). ونظراً لما يشكله هذا الإجراء من مساس بحقوق الأفراد في الخصوصية حيث أنه ينطوي على تجميع وتسجيل البيانات التي يتم نقلها بواسطة نظام معلوماتي معين، فقد تم تحديد الالتزام بتوفير المساعدة المتبادلة المتعلقة بهذا الخصوص، كما أنه يجب أن يكون تقديم المساعدة المتبادلة في الحدود التي تسمح بها المعاهدات والقوانين الداخلية المطبقة لدى الدول الأطراف[1].

ونلاحظ أن هذا الإجراء مماثل مراقبة المحادثات والمراسلات السلكية واللاسلكية أو تسجيل الأحاديث لمصلحة التحقيق والمنصوص عليها في المادة (93) من قانون الإجراءات الجنائية البحريني لسنة 2002 والتي أحاط هذا الإجراء بعدة شروط أهمها أن يتم هذا الإجراء إذا كان له فائدة في ظهور الحقيقة في جناية أو جنحة معاقب عليها بالحبس، وأن يتخذ هذا الإجراء بإذن من قاضي المحكمة الصغرى، وأن يكون قرار ضبط المراسلات أو المراقبة أو التسجيل

-(1) المرجع نفسه- ص 292- 293

مسبباً ولمدة.فضلا عن أن المادة (26) من دستور مملكة البحرين المعدل عام 2002 قد نصت على أن (حرية المراسلة البريدية والبرقية والهاتفية والإلكترونية مصونة، وسريتها مكفولة، فلا يجوز مراقبة المراسلات أو إفشاء سريتها إلا في الضرورات التي يبينها القانون، ووفقا للإجراءات والضمانات المنصوص عليها فيه.)

المطلب الثالث

تسليم المجرمين[1]

يعد نظام تسليم المجرمين من أهم وسائل التعاون الدولي لمكافحة الجرائم المعلوماتية، فإذا كان نظام تسليم المجرمين إجراء احتياطي بالنسبة لكثير من الجرائم التقليدية، يتم اللجوء إليه في حالة فرار الجاني إلى خارج الدولة التي وقعت الجريمة على إقليمها، فإن هذا النظام يعد إجراء رئيساً بالنسبة لمعظم الجرائم المعلوماتية التي يقوم بارتكابها الجاني وهو في دولة وتتحقق الجريمة على إقليم دولة أخرى منتهكاً بذلك قوانينها وأنظمتها الداخلية، لذا فإن الدولة الأخيرة لا يكون أمامها سوى اللجوء إلى نظام تسليم المجرمين لملاحقة ومن ثم محاكمة هذا المجرم عن جريمته تلك أو لتنفيذ حكم صادر من محاكمها ضده في هذا الشأن.

وتنبع أهمية نظام تسليم المجرمين من كونه يحقق مصلحة المجتمع الدولي في مكافحة الجريمة، وذلك من خلال عدم إتاحة الفرصة للمجرم بالإفلات من قبضة العدالة والتي تتحقق في الدولة الطالبة، وضمان معاقبته على ما اقترفه من جرم[2].

---

(1) تعد المعاهدة التي عقدت بين رمسيس الثاني ملك مصر وملك الحيثيين هاتوسيلى عام 1280 قبل الميلاد أو 1300 قبل الميلاد أول معاهدة في التاريخ بصفة عامة وفي مجال تسليم المجرمين بصفة خاصة. وقد تم توقيع هذه المعاهدة بعد المعركة التي دارت بين المملكين والتي عرفت باسم (معركة قادش) المرجع: د. عبدالفتاح محمد سراج – النظرية العامة لتسليم المجرمين – دار النهضة العربية – بدون تاريخ نشر – القاهرة – صـ 10-8

(2) المرجع السابق- صـ 90-91

الفرع الأول

ماهية نظام تسليم المجرمين

أولا: مفهوم تسليم المجرمين:

يعد مصطلح تسليم المجرمين الترجمة العربية لكلمة Extradition () وهي كلمة فرنسية استعملت لأول مرة في مرسوم 19 فيفري 1791 في فرنسا، ولكلمة (extradition)الإنجليزية التي اشتقت من الفرنسية واستعملت لأول مرّة في بريطانيا في قانون التسليم سنة 1870[1].

وقد عرفت المادة (1) من المعاهدة النموذجية لتسليم المجرمين الصادرة بقرار الجمعية العامة للأمم المتحدة رقم (116/45) نظام تسليم المجرمين بأنه (مجموعة الإجراءات القانونية التي تهدف إلى قيام دولة بتسليم شخص متهم أو محكوم عليه إلى دولة آخرى، لكي يحاكم بها أو ينفذ فيها الحكم الصادر عليه من محاكمها)[2]

وتعرفه المحكمة العليا الأمريكية بأنه (الإجراء القانوني المؤسس على معاهدة أو معاملة بالمثل أو قانون وطني، حيث تتسلم دولة ما من دولة آخرى شخص متهم أو مرتكب مخالفة جنائية ضد القوانين الخاصة بالدولة الطالبة، أو مخالفة للقانون الجنائي الدولي، حيث يعاقب على ذلك في الدولة الطالبة)[3] .

ويعرفه البعض بأنه قيام إحدى الدول ويطلق عليها (الدولة المطلوب منها التسليم) بتسليم شخصا موجودا على إقليمها إلى دولة آخرى يطلق عليها (الدولة طالبة التسليم) أو (الطالبة) بناءا على طلبها بغرض محاكمته عن جريمة

(1) بنفرد لطفي لمين – التعاون الدولي في مجال تسليم المجرمين - مجلة الشرطة الجزائرية – العدد 92 أكتوبر 2009 – صـ13

(2) د.رقية عواشرية – نظام تسليم المجرمين ودوره في تحقيق التعاون الدولي لمكافحة الجريمة المنظمة- مجلة المفكر(مجلة علمية محكمة متخصصة في الحقوق والعلوم السياسية) جامعة محمد خضير- الجزائر – بسكرة – العدد الرابع 2008- صـ19

(3) د. عبدالفتاح محمد سراج – مرجع سابق – صـ 55

نسب إليه ارتكابها أو لتنفيذ حكم صادر ضده من محاكمها[1].

كما يعرفه آخرون بأنه تخلي الدولة عن شخص موجود على إقليمها إلى دولة آخرى بناء على طلبها لتحاكمه عن جريمة يعاقب عليها قانونها أو لتنفيذ حكم صادر من محاكمها[2].

وباستعراض التعريفات المتقدمة، نلاحظ أن لا اختلاف فيما بينها على تعريف نظام تسليم المجرمين.

وفي تقديري فإن تعريف المحكمة العليا الأمريكية كان أكثرها توسعا حيث شمل بالتعريف الأساس القانوني لنظام تسليم المجرمين وهو إما معاهدة أو معاملة بالمثل أو القانون الوطني، فضلا عن شموله مخالفة القانون الجنائي الدولي كسبب لتسليم المجرمين، وهو ما نجد تطبيقه في الأحكام أو طلبات تسليم المجرمين الصادرة عن المحكمة الجنائية الدولية بشأن عدد من مرتكبي جرائم دولية مثل الجرائم ضد الإنسانية أو جرائم الحرب وجرائم الإبادة مثال على ذلك، دعوة ممثل الادعاء في المحكمة الجنائية الدولية الحكومة السودانية إلى تسليم وزير سوداني وقائد مليشيا الجنجويد لمحاكمتهما بدعوى ارتكابهما جرائم ضد الإنسانية [3].

ثانيا: طبيعة نظام تسليم المجرمين:

انقسم الفقهاء في تحديد طبيعة نظام تسليم المجرمين إلى ثلاث اتجاهات وبيانهم كالآتي:

1- الطبيعة القضائية؛ يرى أنصار هذا الاتجاه أن تسليم المجرمين عملا من أعمال القضاء هدفه معاقبة المجرم على ما ارتكبه من مخالفة جنائية ضد القوانين الخاصة بالدولة الطالبة، وتبرير ذلك أن الطبيعة القضائية ترتبط

---

(1) د. جميل عبد الباقي الصغير- مرجع سابق صـ 88

(2) سراج الدين محمد الروبي - الانتربول وملاحقة المجرمين -الدار المصرية اللبنانية - القاهرة 1998 - صـ 3

(3)http://www.aljazeera.net/news/pages/2d8100d8-7586-4ef3-9fd5-816934124224

بالسلطة المختصة بالبت في طلب التسليم، وهي السلطة القضائية، فهي من تملك رفض أو قبول التسليم، ويكون قرارها نهائي غير قابل للطعن فيه[1]. كما هو الحال في بريطانيا والولايات المتحدة الأمريكية حيث يتم عرض مسألة التسليم على القضاء الذي يتولى البحث في الأدلة الاتهام المقدمة، حيث تنظر الدعوى وتناقش أمام القضاء حتى ولو كان هناك حكم قد صدر بشأنه، في حين يذهب القضاء في معظم الدول الآخرى إلى عدم بحث الوقائع ويقوم بتطبيق القانون الوطني والمعاهدات الخاصة بالتسليم.[2]

وقد تعرض هذا الاتجاه للنقد على أساس أنه لا يمكن إسباغ الصفة القضائية المحضة على القرار الصادر من السلطة القضائية بالبت في طلب التسليم، لآن نظر طلبات التسليم من قبل السلطة القضائية لا يعتبر محاكمة بالمعنى الفني الدقيق،فالسلطة القضائية عند نظرها طلب التسليم، فأنها لا تباشر هذا العمل من واقع الاختصاص القضائي المحض، وإنما تباشره إعمالا لقواعد السيادة التي يجب أن تراعيها عند نظر طلب التسليم وفقا للاتفاقيات الدولية والتشريعات الوطنية، بصفتها مصادراً أساسياً لنظام تسليم المجرمين. كما أن قرار السلطة القضائية بالموافقة على طلب التسليم لا يلزم السلطة التنفيذية في الدولة، حيث تملك الأخيرة رفض التسليم إذا ما كانت هناك مصلحة سياسية تبرر ذلك[3].

2- الطبيعة السيادية: يرى أنصار هذا الاتجاه أن التسليم هو عمل من أعمال السيادة تباشره الحكومة بإرادتها المنفردة، وفقا للاتفاقيات الدولية والتشريعات الوطنية، التي تشكل المصدر الأساسي لنظام تسليم المجرمين، ويستندون في ذلك إلى أحد أحكام مجلس الدولة الفرنسي الصادر في 30 مايو 1952، والذي أشار إلى أن الأعمال التي تصدر عن الحكومة تعتبر بطبيعتها أعمالاً إدارية تدخل في نطاق أعمال السيادة التي تحرر الدولة من قواعد

---

(1) بلفرد لطفي لمين - مرجع سابق - صـ 14

(2) د.رقية عواشرية - مرجع سابق صـ 20

(3) د. عبدالفتاح محمد سراج - مرجع سابق - صـ 96 - 97

المشروعية، والتسليم يعتبر من أعمال السيادة الذي تمارسه الدولة بإرادتها المنفردة ممثلة في أجهزتها الحكومية والتنفيذية.

وقد انتقد هذا الاتجاه، على أساس أنه استند إلى أحد أحكام مجلس الدولة الفرنسي القديمة التي لا تعكس الموقف الحالي للمجلس الذي يسبغ الصفة القضائية على قرار التسليم، حيث أعطت الحق لكل من الشخص المطلوب تسليمه والدولة الطالبة الطعن على القرار الصادر بالتسليم، فضلا عن تعارض نظام تسليم المجرمين وفقاً لهذا الاتجاه مع مبدأ سيادة الدولة على إقليمها حيث يعد انتهاكا لحق الدولة في حماية الأشخاص المقيمين على أرضها ولا يمكن تشجيع الدول على مبدأ التسليم[1].

3- الاتجاه المختلط: يرى أنصار هذا الاتجاه أن نظام تسليم المجرمين يتمتع بطبيعة مزدوجة، فهو من جهة يعتبر عملا قضائياً من حيث الإجراءات التي يقوم بها القضاء، في إصدار أوامر القبض والتحقيق وإصدار قرار التسليم، والتي جميعها تهدف إلى معاقبة الجاني. ومن جهة أخرى فإن القرار النهائي لقبول التسليم، أو رفضه يبقى للسلطة السياسية ويصبح دور القضاء استشارياً[2].

- ولقد نظم المشرع البحريني موضوع تسليم المجرمين، في الفصل الأول من الباب الثاني من قانون الإجراءات الجنائية لعام 2002 وذلك بالمواد من (412) إلى (425)، وباستقراء تلك النصوص نلاحظ أن المشرع البحريني قد تبنى الاتجاه المختلط فيما يتعلق بطبيعة نظام تسليم المجرمين ومظاهر ذلك أنه وفقا للمواد المشار إليها فإن السلطة القضائية ممثلة في المحكمة الكبرى الجنائية تختص بالنظر في طلبات التسليم وفي استيفاء شرائطه وإجراءاته، وتصدر المحكمة قرارها مسبباً في طلب التسليم، ثم تحيله إلى السلطة التنفيذية ممثلة في وزير العدل، حيث يكون له القرار النهائي

---

(1) المرجع نفسه – صـ 93 - 95

(2) بلفرد لطفي لمين – مرجع سابق – صـ 14

بشأن إصدار قراراً بالتسليم أو الامتناع عنه.

ومن جانبي أرى أن نظام تسليم المجرمين إما أن يكون قضائيا، وإما يكون عملاً من أعمال السيادة وذلك في ضوء وجود قوانين أو اتفاقيات مصدقا عليها من قبل الدولة من عدمه، وبيان ذلك كالآتي:

1- يكون نظام تسليم المجرمين قضائيا، إذا ما كان مصدره القانون الداخلي للدولة المقدم إليها طلب التسليم أو المعاهدات أو الاتفاقيات الدولية أو الثنائية التي لها قوة القانون المصدقة عليها هذه الدولة، وليس في ذلك مساس بسيادة الدولة، إذ أنه بما لها من سيادة أبرمت الاتفاقيات الدولية والثنائية ومنحتها قوة القانون، وأنها بذلك قد خولت السلطة القضائية والمناط بها تطبيق القانون الاختصاص بالبت في طلبات التسليم.و قد ينظر إلى رفض السلطة السياسية تنفيذ طلب التسليم على الرغم من قرار السلطة القضائية بتحقق شروطه قرينة على إخلال الدولة بالتزاماتها في الوفاء بتعهداتها الدولية. بالإضافة إلى ما قد يشكله من عدم احترام لأحكام القضاء.

ومن جانب آخر أن اعتبار التسليم عملا قضائيا تنفذه الدولة بناء على القرار الصادر عن السلطة القضائية متى تحققت شروطه، يساعد على تحقيق الهدف من نظام تسليم المجرمين وهو مكافحة الجريمة على مستوى الدول وحتى لا يكون العالم مكاناً آمناً للمجرمين، حيث أنه مجرد الخلاف بين الدول قد يعوق تنفيذه، ويفتح المجال أمام المجرمين لاستغلاله، والإفلات من العقاب، فقد يقصد مجرم ما الفرار إلى دولة ليست على وفاق مع الدولة التي ارتكب فيها جريمته، حتى يستغل التوتر القائم بينهما لعدم تسليمه وبالتالي تمكنه من الفرار.

2- بينما يكون التسليم عملا من أعمال السيادة، خاصة في حالة غياب الاتفاقيات الدولية أو الثنائية، فإن القرار النهائي لقبول التسليم أو رفضه يبقى للسلطة السياسية، وفقا للاعتبارات المصلحة العامة والاعتبارات

السياسية التي تحيط بقرارها.

وتجدر الإشارة إلى أنه في حالة غياب المعاهدات الدولية أو الاتفاقيات الثنائية بين الدولة الطالبة أو المقدم إليها الطلب، فإن تسليم المجرمين قد يستند إلى شرط المعاملة بالمثل، وقواعد المجاملات الدولية كما سنبينه لاحقاً بمناسبة تناول مصادر التسليم المجرمين .

الفرع الثاني

مصادر نظام تسليم المجرمين

تتعدد مصادر نظام تسليم المجرمين والتي على أساسها تطلب إحدى الدول من دولة آخرى تسليم شخص مقيم على إقليمها إليها لمحاكمته أو تنفيذ حكم قضائي صادر بحقه، وتنقسم هذه المصادر إلى نوعين مصادر أصلية والتي تستند إليها الدول الأطراف في عملية التسليم لإتمام إجراءات التسليم،ومصادر احتياطية والتي عادة ما تلجأ إليها الدول عندما يصعب الاعتماد على المصادر الأصلية، أو في حالة غيابها. وسنتولى بيان تلك المصادر على النحو الآتي:

1- المصادر الأصلية وتشمل:

أ- المعاهدات والاتفاقيات بين الدول:

تعرف المعاهدات الدولية بأنها (اتفاق مكتوب ما بين شخصين أو أكثر من أشخاص القانون الدولي العام، لإحداث آثار قانونية معينة وفقاً لأحكام القانون الدولي العام)[1]

وتعد المعاهدات والاتفاقيات بين الدول أحد أهم مصادر نظام تسليم المجرمين، حيث أنه في ظل غياب معاهدة دولية ملزمة بشأن تسليم المجرمين فأنه لا يمكن القول بوجود التزام دولي بتسليم المجرمين. ولقد شهد العالم بعد الحرب العالمية الثانية زيادة في عدد المعاهدات الدولية، والثنائية، ومتعددة الأطراف لتنظيم إجراءات تسليم المجرمين ومن الأمثلة على هذه الاتفاقيات اتفاقية جامعة الدول العربية لتسليم المجرمين 1952، والاتفاقية الأوربية المتعلقة بتسليم المجرمين 1957م وبروتوكولاتها الإضافية (1975- 1978)، و اتفاقية المنظمة المشتركة لأفريقيا ومدغشقر 1961، وخطة الكومنولث لتسليم المجرمين 1966م. واتفاقية الرياض العربية

---

(1) د. علي خليل أسماعيل الحديثي- القانون الدولي العام – ج (1) المبادئ والأصول – دار النهضة العربية – القاهرة 2010 – ص31

للتعاون القضائي 1983م والاتفاقية الأمنية الخليجية 1994م، واتفاقية تبسيط إجراءات تسليم المجرمين بين الدول الأعضاء في الاتحاد الأوربي، واتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية 2000م[1]، وكذلك بالإضافة إلى اتفاقية بودابست المتعلقة بالجريمة الإلكترونية لسنة 2001 والتي تضمنت أحكاماً خاصة بتسليم المجرمين في المادة (24) منها. وكذلك الاتفاقية العربية لمكافحة جرائم تقنية المعلومات 2010 والتي تضمنت أحكاماً خاصة بتسليم المجرمين في المادة (31) منها.

وفي هذا السياق فقد قامت مملكة البحرين بالانضمام إلى عدة اتفاقيات دولية وإقليمة وثنائية لتنظيم إجراءات تسليم المجرمين، أبرزها اتفاقية تسليم المجرمين بين دول الجامعة العربية 1952، وصادقت عليها بموجب المرسوم الأميري رقم (21) لسنة 1973، واتفاقية الرياض العربية للتعاون القضائي لعام 1983، وصادقت بموجب المرسوم بقانون رقم (41) لسنة 1999. واتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية والبروتوكولين المكملين لها بموجب القانون قم (4) لسنة 2004، والاتفاقية العربية لمكافحة جرائم تقنية المعلومات 2010 والتي تضمنت أحكاماً خاصة بتسليم المجرمين في المادة (31) منها. كما أبرمت اتفاقية التعاون القضائي والقانوني في المواد المدنية والتجارية والجزائية والأحوال الشخصية وتسليم المجرمين وتصفية التركات مع الجمهورية العربية السورية والتي صادقت عليها بموجب المرسوم بقانون رقم (30) لسنة 2001، كما أبرمت اتفاقية وحكومة جمهورية الهند والتي صادقت عليها بموجب القانون رقم (10) لسنة 2005.[2]

وفي مثال عملي يوضح أهمية التعاون الدولي في مجال تبادل وتسليم المجرمين لمكافحة الجرائم المعلوماتية بشكلٍ عام والجرائم الماسة بسرية

---

(1) منتدى نادي قضاة مصر http://egyptjudgeclub.org/forum/showthread.php?tid=3048

(2) نصوص الاتفاقيات التي صادقت عليها مملكة البحرين في مجال تسليم المجرمين منشورة على الموقع الإلكتروني لهيئة التشريع والإفتاء القانوني بمملكة البحرين /http://www.legalaffairs.gov.bh

المعلومات الإلكترونية بشكلٍ خاص، شن شاب من روسيا في تسعينات القرن الماضي هجوماً إلكترونيا على سيتي بنك حيث تمكن من النفاذ بشكل غير مسموح به إلى وحدة خدمة المصرف في الولايات المتحدة. وقد استعان هذا الشاب بعدد من الأشخاص لفتح حسابات في فروع المصرف في شتى أنحاء العالم، ثم أصدر تعليمات لحاسوب المصرف بتحويل أموال إلى تلك الحسابات. وعندما انكشف المخطط وتم تحديد هوية الفاعل ، وصدر أمر بالقبض عليه من المحكمة الاتحادية بالولايات المتحدة. ولم يكن هناك آنذاك معاهدة لتسليم المجرمين بين روسيا والولايات المتحدة، إلا أن المتهم قام بزيارة المملكة المتحدة لحضور معرض عن الحاسوب. وبموجب اتفاقات التسليم القائمة بين المملكة المتحدة والولايات المتحدة تمكنت السلطات البريطانية من تقديم المساعدة ، وطلب المتهم أن تنظر المحكمة في قانونية توقيفه للطعن في تسليمه وساق حججا منها أن أمر تحويل الأموال قد صدر في روسيا، حيث توجد لوحة مفاتيح حاسوبه وليس في الولايات المتحدة. واعتبرت المحكمة أن الوجود المادي للمتهم في سانت بطرسون - روسيا أقل أهمية من أن فعله الإجرامي قد تم على أقراص مغناطيسية موجودة في الولايات المتحدة. فضلا عن التهم التي وجهت للمتهم كان لها مقابل واضح في القانون البريطاني الخاص بإساءة استخدام الحاسوب لعام 1990؛ فلو أتى المتهم سلوكه الإجرامي من المملكة المتحدة بدلا من روسيا لكان للمحاكم البريطانية الاختصاص القضائي. وتم تسليم المتهم إلى الولايات المتحدة حيث صدر حكم بإدانته وسجنه[1].

ونظراً لأهمية وفاعلية نظام تسليم المجرمن في مكافحة الجريمة، فإنه ولضمان الاستفادة منه في مجال مكافحة الجريمة المعلوماتية فقد نصت الفقرة (3) من المادة (24) من اتفاقية بودابست المتعلقة بالجريمة الإلكترونية 2001 على أن أي دولة طرف لا توافق على تسليم المجرمين، سواء لأنه لا

---

(1) ورقة عمل بعنوان (تدابير لمكافحة الجرائم المتصلة بالحواسيب) مقدمة في مؤتمر الامم المتحدة الحادي عشر لمنع الجريمة والعدالة الجنائية - مرجع سابق - صـ 8-9

يوجد اتفاق مبرم مع الطرف طالب التسليم، أو لأن الاتفاق المبرم بينهما لا يشمل التسليم بالنسبة للجرائم المعلوماتية الواردة بالاتفاقية والتي من بينها الجرائم الماسة بسرية المعلومات الإلكترونية وهي الدخول غير القانوني للنظام المعلوماتي، والاعتراض غير القانوني للبيانات، فإنه في هذه الحالة يمكن اعتبار اتفاقية بودابست كأساس قانوني لتسليم الشخص المطلوب تسليمه على الرغم من أن هذا الطرف غير ملزم بذلك[1].ولقد نصت الاتفاقية العربية لمكافحة جرائم تقنية المعلومات 2010 على ذات الحكم في الفقرة (3) من المادة (31) منها[2].

ب- القانون الداخلي:

بالإضافة إلى عقد العديد من الاتفاقيات الإقليمية والدولية والثنائية التي تعنى بعملية التسليم، فقد حرصت معظم الدول على تنظيم أحكام تسليم المجرمين إما من خلال تشريعاتها الجزائية مثل الولايات المتحدة الأمريكية حيث ينظم قانونها الفدرالي الأحكام العامة لإجراءات التسليم إلى جانب تشريع كل ولاية، وقانون الإجراءات الجنائية الإيطالي لسنة 1988، وقانون الإجراءات الجنائية البولندي لسنة 1969، ومن التشريعات العربية، قانون الإجراءات الجنائية العراقي والتونسي والجزائري. وبذات الاتجاه أخذ المشرع البحرين، حيث نظم أحكام تسليم المجرمين قانون الإجراءات البحريني لعام 2002 مسألة تسليم المجرمين كما سبق ألإشارة في الفصل الأول من الباب الثاني وذلك بالمواد من (412) إلى (425). وقد تقوم بعض الدول بسن تشريعات خاصة بتسليم المجرمين، مثل قانون تسليم المجرمين الانجليزي لسنة 1989، والقانون الفرنسي لعام 1927، ومن التشريعات

---

(1)د. هلالي عبداللاه أحمد – كيفية المواجهة التشريعية لجرائم المعلوماتية في النظام البحريني على ضوء اتفاقية بودابست – مرجع سابق – صـ 249

(2) تنص الفقرة (3) من المادة (31) من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات 2010 على أنه (إذا قامت دولة طرف ما بجعل تسليم المجرمين مشروطاً بوجود معاهدة وقامت باستلام طلب لتسليم المجرمين من دولة طرف أخرى ليس لديها معاهدة تسليم فيمكن اعتبار هذه الاتفاقية كأساس قانوني لتسليم المجرمين فيما يتعلق بالجرائم المذكورة في الفقرة (1) من هذه المادة)

العربية، القانون العماني 2000/4م، وقانون تسليم المجرمين الأردني لعام 1927.

ج - العرف الدولي:

يعد العرف الدولي من الناحية التاريخية أقدم مصادر القاعدة الدولية وهو في المرتبة الثانية بعد المعاهدات حسب ترتيب المادة 38 من النظام الأساسي لمحكمة العدل الدولية.

والعرف الدولي هو عبارة عن مجموعة من الأحكام أو القواعد القانونية نشأت من تكرار التزام الدول بها وإتباعها في تصرفاتها مع غيرها في مناسبات معينة بوصفها قواعد ملزمة في اعتقاد غالبية الدول[1].

ويعتبر العرف الدولي في مجال تنظيم تسليم المجرمين مصدراً أساسياً استقت منها المعاهدات والتشريعات الوطنية أحكامها. ومن أبرز القواعد العرفية غب مجال تسليم المجرمين وتضمنتها الاتفاقيات الدولية والتشريعات الوطنية، هي شرط التجريم المزدوج، ومبدأ الخصوصية، واستثناء تسليم الرعايا، وحظر تسليم اللاجئ، وعدم جواز التسليم في الجرائم السياسية[2].

ويعد من أبرز قواعد العرف الدولي في مجال تسليم المجرمين ، حالة عدم جواز تسليم رؤساء وملوك الدول الأجنبية لتمتعهم بحصانة تحول دون خضوعهم لنطاق إقليمية القاعدة الجنائية،عما يرتكبونه من جرائم على هذا الإقليم. وعليه فإنه إذا ارتكب أحد رؤساء الدول جريمة خارج دولته وتوجه إلى دولة آخرى، فأنه لا يجوز للدولة الأخيرة أن تقوم بتسليمه وتشمل هذه الحصانة أفراد أسرة رئيس أو ملك الدولة وحاشيته. وجدير بالذكر أن هذه الحصانة لا تحول دون طلب تسليم أحد رؤساء أو ملوك الدول في حالة ارتكابهم أحد الجرائم الدولية التي تدخل في نطاق اختصاص

---

(1) د. علي خليل أسماعيل الحديثي – مرجع سابق- صـ 81

(2) د. عبدالفتاح محمد سراج – مرجع سابق- صـ 140

المحكمة الجنائية الدولية[1]، وذلك استناداً إلى المادة (27) من نظام روما الأساسي حيث تنص على أنه (1- يطبق هذا النظام الأساسي على جميع الأشخاص بصورة متساوية دون أي تمييز بسبب الصفة الرسمية. وبوجه خاص، فإن الصفة الرسمية للشخص، سواء كان رئيساً لدولة أو حكومة أو عضواً في حكومة أو برلمان أو ممثلا منتخباً أو موظفاً حكومياً، لا تعفيه بأي حال من الأحوال من المسؤولية الجنائية بموجب هذا النظام الأساسي، كما أنها لا تشكل، في حد ذاتها، سببا لتخفيف العقوبة. 2- لا تحول الحصانات أو القواعد الإجرائية الخاصة التي قد ترتبط بالصفة الرسمية للشخص، سواء كانت في إطار القوانين الوطنية أو الدولية، دون ممارسة المحكمة اختصاصها على هذا الشخص.)

وقد عد قانون الإجراءات البحريني لسنة 2002 العرف الدولي من بين مصادر الأساسية نظام تسليم المجرمين وفقاً للمادة (412)، حيث نصت تلك المادة على اللجوء لقواعد القانون الدولي العام فيما لم يرد في شأنه نص خاص في المعاهدات والاتفاقيات الدولية التي لها قوة القانون في مملكة البحرين، أو قانون الإجراءات الجنائية.

2- المصادر الاحتياطية وتشمل:

أ- **المعاملة بالمثل:**

تعد المعاملة بالمثل أحد أهم الأدوات في مجال العلاقات الدولية ، وللمعاملة بالمثل جذور تاريخية بعيدة، فقد عرفها البابليون ونص عليها تشريع حمورابي (المواد 196 ـ 200)، كما عرفها الإغريق والقبائل العربية[2].

قد يحدث أن يكون مرتكب الجريمة المعلوماتية يقيم في دولة لا تربطها اتفاقيات تبادل تسليم المجرمين، ففي هذه الحالة قد تلجأ الدولة الطالبة إلى

---

(1) مرجع سابق – صـ 227- 228

(2) الموسوعة العربية :

http://www.arab-ency com/index php?module=pnEncyclopedia&func=display_term&id=160697

مبدأ المعاملة بالمثل كأساس للمطالبة بالتسليم، وعادة ما يتحقق ذلك من خلال تضمين قرار التسليم الصادر عن الدولة المطالبة بالتسليم، الإشارة إلى تعهد الدولة الطالبة، معاملة طلبات الدولة المطلوب منها التسليم نفس المعاملة،وتقوم الدول عادة بحفظ خطاب التسليم مرفقا به تعهد الدولة طالبة التسليم بمعاملة طلبات الدولة المطلوب منها التسليم بالمثل، حتى يمكن الرجوع إليها في وقت الحاجة، كما يتم عادة إخطار إنتربول الدولة طالبة التسليم أن التسليم سيتم استناداً إلى المبدأ المعاملة بالمثل وفي ظل الشروط الواردة في طلب الدولة طالبة التسليم حتى يمكن تبادل المعلومات مستقبلا في ضوء هذه المتغيرات[1].

وفي تطبيق عملي لهذا المبدأ في مجال تسليم المجرمين ، قامت جمهورية مصر العربية بإبرام مذكرة تفاهم لتسليم المجرمين على أساس المعاملة بالمثل مع الولايات المتحدة الأمريكية، تتعهد فيها الخبرة بإتباع سلوك مماثل مع مصر بعد موافقتها على تسليم أحد المجرمين والذي يحمل الجنسية الإسرائيلية إلى الولايات المتحدة لأمريكية، متهم في جريمة جلب مخدرات من الهند إلى الولايات المتحدة الأمريكية بالإضافة إلى اتهامه بقتل أحد ضباط جهاز مكافحة المخدرات الأمريكي[2].

ب- قواعد المجاملات والأخلاق الدولية:

تعرف قواعد المجاملات الدولية، بأنها تلك القواعد التي اعتادت الدول على إتباعها، رغبة منها في توطيد علاقاتها مع بعضها البعض، ولا تحمل هذه القواعد صفة الإلزام ومن أمثلتها مراسم استقبال رؤساء الدول والسفراء والتحية البحرية[3].

---

(1) سراج الدين محمد الروبي – مرجع سابق – صـ 46.

(2) د. عبدالفتاح محمد سراج – مرجع سابق- صـ 157

(3) د. علي خليل أسماعيل الحديثي – مرجع سابق- صـ 10

وعلى الرغم من أن تلك القواعد غير ملزمة قانوناً إلا أنها تتمتع بصفة الإلـزام الأدبي، حيث أنها تكتسب أهميتها من كونها توطد من علاقـات الـدول ببعضـها، وبالتـالي فـإن الإخلال بها يؤدي نتيجة عكسية، حيث سيقابل إخلال الدولـة بقواعـد المجـاملات تجـاه دول آخرى ، إخلال مقابل من تلك الأخيرة من باب المعاملة بالمثل.

ويمكن الاستناد إلى قواعد المجاملات الدولية في مجال تسليم المجرمين في حال غيـاب اتفاقيات تسليم بين الدولة الطالبة والدول المطلوب منها التسليم، حيث تقوم دولـة مـا في سبيل توطيد علاقاتها بدولة آخرى أو تعزيزها، تنفيذ طلب التسليم المقدم إليهـا مـن دولة آخرى دون يربطهما اتفاقية تبادل تسليم المجرمين.

ومن التطبيقات العملية على عمليات التسليم التي تمت على أساس قواعد المجاملـة الدولية، فقـد قامـت الولايـات المتحـدة الأمريكيـة في عـام 1962م بطلـب تسـليم أحـد المتهمين في قضية مخدرات من جمهورية لبنان، على الرغم من عدم ارتباطهما بمعاهـدة تسليم حينها، وقد تأسس الطلب الأمريكي على قواعد المجاملة الدولية[1].

أما قواعد الأخلاق الدولية بأنها مجموعة من المبـادئ السـامية التـي يمليهـا الضـمير العالمي ويقيد بها تصرفـات الـدول وفقـاً لمعـايير الأخـلاق الفاضـلة والمـروءة والشـهامة، ولكنها ليست ملزمة من الناحية القانونية، ومن أمثلة عـلى تلـك القواعـد الابتعـاد عـن الكذب والخداع في العلاقات الدولية، وتقديم العون والغوث إلى الدول المنكوبة[2].وهذه القواعد هي آخرى ذات إلزام أدبي.

---

(1) د. عبدالفتاح محمد سـراج – مرجع سابق- صـ 167

(2) د. علي خليل أسماعيل الحديثي – مرجع سابق- صـ 11

الفرع الثالث

شـروط تسليم المجرمين

سنتناول في هذا الفرع شـروط التسليم والشـروط المتعلقة بالأشخاص المطلوب تسليمهم بالإضافة إلى الشـروط المتعلقة بالجريمة المطلوب التسليم بشأنها، وذلك على النحو الأتي:

أولا: الشـروط المتعلقة بالجريمة:

1- أن تكون الجريمة قد ارتكبت في إقليم الدولة طالبة التسليم ، أو ارتكبت خارج إقليمها وكانت قوانينها تعاقب على ذلك، مثال الجرائم الماسة بأمن الدولة الاقتصادي أو السياسي أو العسكري التي تنص غالبية التشـريعات على معاقبة مرتكبيها ولو وقعت خارج إقليمها. مثال على ذلك المادة (6) من قانون العقوبات 1976 والتي تنص على أنه (تسـري أحكام هذا القانون على كل مواطن أو أجنبي ارتكب خارج دولة البحرين عملا يجعله فاعلا أو شـريكا في جناية من الحنايات الماسة بأمن الدولة الخارجي أو الداخلي المنصوص عليها في الفصلين الأول والثاني من الباب الأول من القسم الثاني أو في جناية تقليد الأختام والعلامات العامة أو تزييف العملة وأوراق النقد المنصوص عليها في المواد 257 ، 262 ، 263 .)

ونظراً لطبيعة الجرائم المعلوماتية عابرة الحدود فإن كثير من المشـرعين يحرصون على تضمين التشـريعات الخاصة بمكافحة الجرائم المعلوماتية نصوص تمد سريان أحكام تلك القوانين على الجرائم المعلوماتية التي ترتكب كليا أو جزئيا تقع خارج إقليمها إضراراً بمصالحها، ومن أمثلتها نص المادة (2) من قانون مكافحة جرائم تقنية المعلومات 2011 (تسـري أحكام هذا القانون على جرائم تقنية المعلومات ولو ارتكبت كلياً أو جزئيا خارج السلطنة متى أضرت بأحد مصالحها، أو إذا تحققت النتيجة الإجرامية في إقليمها أو كان يراد لها أن تتحقق فيه ولو لم تتحقق.)

2- التجريم المزدوج [1]، ويقصد به أن يكون الفعل المرتكب، الذي يستند إليه الطلب، يشكل جرما إذا ارتكب في أراضى الدولة المطالبة[2]. بعبارة آخرى أن يكون الفعل المطلوب التسليم من أجله مجرّما في تشريع الدولة طالبة التسليم ، وكذلك في تشريع الدولة المطلوب منها التسليم.

ويتحقق التجريم المزدوج، إذا ما كان الفعل مجرّما بأي صورة كانت، ولا عبرة بالوصف أو التكيف القانوني الذي يطلق على الفعل عند تقرير توافر هذه الشروط والمعاقبة عليه، حيث أنه قد تختلف تشريعات الدول في التكيف القانوني الذي توصف فيه الجريمة فمثلا لو كان الفعل معاقبا عليه في تشريع الدولة الطالبة التسليم تحت مسمى جريمة توظيف الأموال ، بينما كان الفعل نفسه معاقبا عليه تحت مسمى جريمة النصب والاحتيال في الدولة المطلوب منها التسليم، فإن ذلك لا يمنع من توافر شرط ثنائية التجريم أو ازدواجيته [3].ومن الأمثلة على ذلك، إطلاق بعض الدول مثل المغرب والجزائر مصطلح (المحاولة) على الشروع في الجريمة، بينما تستخدم بعض الدول الآخرى مصطلح (الشروع) مثل مملكة البحرين، ومصر، والعراق.

وشرط التجريم المزدوج يجد أساسه في أن نظام تسليم المجرمين إنما شرع لأجل تمكين الدولة طالبة التسليم من محاكمة من نسب إليه ارتكاب جريمة على إقليمها أو لتنفيذ العقوبة المحكوم بها عليه والصادرة عن محاكمها، وهذا يفترض بداهة أن يكون السلوك موضوع طلب التسليم مجرّم في تشريعها، حيث أنه إذا لم يكن مجرّما فلا يتصور وجود دعوى جنائية أو ملاحقة جزائية ضد الشخص المطلوب تسليمه كما لا يتصور قيام حكم جزائي يقضي بعقوبة عليه، هذا من ناحية ، ومن ناحية آخرى فإنه لا يجوز مطالبة الدولة المقدم

---

(1) ولقد أوردت غالبية الاتفاقيات والمعاهدة المتعلقة بتسليم المجرمين مثل هذا الشرط مثل المادة الثانية من المعاهدة النموذجية للأمم المتحدة بشأن تسليم المجرمين ، والمادة الثالثة من اتفاقية جامعة الدول العربية لتسيم المجرمين، و المادة (40) من اتفاقية الرياض العربية للتعاون القضائي

(2) المادة (6) معاهدة الأمم المتحدة النموذجية نموذجية بشأن نقل الإجراءات في المسائل الجنائية 1990

(3) سراج الدين محمد الروبي مرجع سابق ص 53

إليها طلب التسليم بإيقاع عقوبة على ارتكاب سلوك هو في الأساس غير مجرم وفقا لقانونها[1].

كما يبرر هذا الشرط ، أن مبدأ المعاملة بالمثل الذي يقوم على تبادل المصالح بين الدول، وان انعدام التجريم في قانون إحدى الدولتين الطالبة للتسليم، أو المطلوب منه ذلك لا يجعل المبدأ مبرراً لغاية المصلحة الذي يجب أن يقوم من أجلها، فضلاً عن أن هذا الشرط يأتي تحقيقاً لمبدأ المشروعية والذي يقضي بأنه لا جريمة ولا عقوبة إلا بنص.

وفي المثال الذي سقناه من قبل بشأن الهجوم الذي شنه شاب روسي على مصرف سيتي بنك. فكان رد المحكمة على دفع المتهم بعدم جواز التسليم بأن التهم التي وجهت للمتهم كان لها مقابل واضح في القانون البريطاني الخاص بإساءة استخدام الحاسوب لعام 1990؛ بحيث لو ارتكب المتهم سلوكه الإجرامي في المملكة المتحدة بدلا من روسيا كانت المحاكم البريطانية ستكون هي المختصة، وعلى هذا الأساس تم تسليم المتهم إلى الولايات المتحدة حيث صدر حكم بإدانته وسجنه.

ولقد نصت الفقرة (ب) من المادة (413) قانون الإجراءات الجنائية البحريني لسنة 2002 على هذا الشرط بقولها (يشترط للتسليم ....أن تكون الجريمة جناية أو جنحة معاقباً عليها في كل من قانون مملكة البحرين وقانون الدولة طالبة التسليم بالحبس مدة سنة على الأقل أو أن يكون المطلوب تسليمه عن هذه الجريمة محكوماً عليه بالحبس مدة ستة أشهر على الأقل.)

ويتضح من النص السابق أن المشرع البحريني لم يكتف بالنص على شرط التجريم المزدوج في كلا البلدين ، بل اشترط أن تكون الجريمة المطلوب من أجلها التسليم من نوع الجنايات أو الجنح المعاقب عليها بالسجن مدة لا تقل عن سنة وفقا لقانون العقوبات البحريني، وفي حالة أن

---

(1) د.حسين بن سعيد بن سيف الغافري- مرجع سابق- صـ 28

المطلوب تسليمه كان محكوما عليه فأنه يشترط أن تكون العقوبة المحكوم بها عن الحبس لمدة ستة أشهر.

وتجدر الإشارة إلى أن القصور أو الفراغ التشريعي في مجال تجريم الجرائم المعلوماتية في بعض الدول قد يفوت الفرصة على كثير من الدول في الاستفادة من نظام تسليم المجرمين على الرغم من أهميته بالنسبة لمكافحة هذه الجرائم، وذلك لاصطدامه بمبدأ التجريم المزدوج، وهو ما تبدو معه الحاجة الملحة إلى الإسراع في تجريم تلك الجرائم سواء عن طريق تعديل القوانين العقابية القائمة أو بسن تشريعات خاصة لهذا الغرض.

ثانياً: الشروط المتعلقة بالأشخاص المطلوب تسليمهم:

1- عدم جواز تسليم مواطني الدولة المطلوب منها التسليم: حيث أنه من المبادئ السائدة والمستقر عليها في المجتمع الدولي والتي نصت عليها معظم التشريعات الوطنية والاتفاقيات مبدأ عدم جواز تسليم الرعايا أيا كان نوع الجريمة المرتكبة من قبلهم في أي إقليم خارج دولتهم. وعلى ذلك نصت المادة (415) من قانون الإجراءات الجنائية البحرين (لا يجوز التسليم في الحالات الآتية :أ ـ إذا كان المطلوب تسليمه من مواطني مملكة البحرين...) وعليه فإنه إذا ما طلبت إحدى الدول من مملكة البحرين بتسليم أحد مرتكبي الجرائم المعلوماتية، فإنه يمكنها الاستناد إلى هذا الشرط في رفض طلب التسليم.

2- عدم جواز اللاجئين السياسيين: حيث أنه من القواعد المستقر عليها نطاق العرف الدولي وفي غالبية التشريعات والاتفاقيات الدولية والإقليمية والثنائية المتعلقة بتسليم المجرمين عدم جواز تسليم ممنوحي حق اللجوء السياسي.

3- عدم جواز تسليم ممن تمت محاكمتهم عن ذات الجريمة المطلوب تسليمهم لأجلها: متى ما كان الشخص المطلوب تسليمه قد سبقت محاكمته عن الجريمة المطلوب تسليمه لأجلها فبرأ أو عوقب عنها فأنه لا يجوز تسليمه

، ليس هذا فحسب بل أنه أيضا لا يجوز التسليم متى ما كان قيد التحقيق والمحاكمة عن ارتكابه فعلا ما هو ذاته المطلوب تسليمه لأجله. ويعد هذا الشرط من الضمانات الأساسية عند محاكمة الشخص المطلوب تسليمه ويهدف إلى توفير أكبر قدر ممكن من الحماية القضائية للشخص المطلوب تسليمه في الدولة الطالبة، وذلك حتى لا يتعرض هذا الشخص لعقوبة مزدوجة.

المبحث الثاني

الجهود التشريعية لحماية المعلومات الإلكترونية ومواجهة الجرائم الماسة بسريتها

تشكل الجرائم المعلوماتية بوجه عام والجرائم الماسة بسرية المعلومات الإلكترونية بوجه خاص تهديدا خطيراً لأمن المجتمعات سواء على المستوى الدولى أو الوطني، وقد استعرضنا في المبحث السابق أهمية التعاون الدولى لمكافحة هذه الجرائم، وأهم مجالات هذا التعاون. وفي هذه المبحث سنتناول أهم الجهود التشريعية الدولية والإقليمية والوطنية لمكافحة تلك الجرائم وذلك على النحو الآتي:

المطلب الأول

الجهود التشريعية الدولية والإقليمية لحماية المعلومات الإلكترونية ومواجهة الجرائم الماسة بسريتها

يعتبر الفراغ أو القصور التشريعي أحد أهم التحديات الرئيسة في مجال مكافحة الجرائم المعلوماتية بوجه عام ، حيث إن مبدأ الشرعية الجنائية يفرض عدم جواز التجريم والعقاب دون نص. الأمر الذي يحول دون مجازاة مرتكبي الفعل الضار أو الخطر على أمن المجتمع المعلوماتي؛ طالما أن المشرع الجنائي لم يقم بسن التشريعات اللازمة لإدخال هذا الفعل ضمن دائرة التجريم والعقاب.

وفي مثال عملي على ما تقدم، فقد تم عقد جلسة محاكاة لمحاكمة واقعية لأحد قراصنة الانترنت المشهورين خلال مؤتمر الشرق الأوسط الثالث لأمن المعلومات الذي تنظمه أكاديمية الاتصالات في دبي بمشاركة خبراء دوليين ومشاركة عدد من دول الشرق الوسط والاتحاد الأوروبي والولايات المتحدة الأمريكية، حيث تتلخص وقائع القضية عندما تقدمت إحدى شركات المقاولات الكبرى - وسنرمز إليها بـ(أ) - بعطاء للظفر بمناقصة

مشروع ضخم، ولما علمت إحدى الشركات المنافسة لها - وسنرمز إليها بـ (ب) - بذلك بادرت إلى الاتصال بأحد القراصنة (هاكر) المحترفين، وهو شاب أمريكي يبلغ من العمر(26) عاما، حيث قام الأخير مقابل مبلغ من المال باختراق موقع الشركة (أ) وتسلل إلى ملفاتها وتمكن من الوصول إلى الملف الخاص بالمناقصة من خلال التسلل إلى الكومبيوتر الشخصي لمهندس أنظمة الشبكات داخل الشركة (أ)، وبذلك تمكنت الشركة (ب) التي استعانت بالقرصان من الاطلاع على عطاء منافستها، وبالتالي الإسراع بتقديم عطاء أقل بقليل من عطائها لتفوز بالمشروع الضخم الذي بلغت قيمته 20 مليون دولار. وفي أعقاب ذلك قامت الشركة الضحية بقرار من مجلس إدارتها باللجوء إلى الشرطة التي أتت إلى مسرح الجريمة وراجعت المعلومات المسروقة في سجلات الشركة بواسطة خبراء مدربين تدريبا عالياً في تقنية المعلومات فأكدت الشرطة وقوع الجريمة، واستطاعت تقفي أثر القرصان باستخدام أساليب تقنية حديثة،وإحالته إلى القضاء.وقد تم في جلسة المحاكاة محاكمة القرصان وفقا للقانونين الإماراتي والأمريكي وذلك بحضور قضاة من الولايات المتحدة الأمريكية ومصر والإمارات، وقد جرت في هذه المحاكمة مساجلات كثيرة تمحورت حول ما إذا كان السطو على المعلومات جريمة مكتملة الأركان إذا تسببت في خسائر مادية للطرف المتضرر بالرغم من غياب أدلة مادية ملموسة وبعد إجراءات التحقيق والمحاكمة المثيرة خلص القاضي الأمريكي إلى إدانة المتهم بالجريمة المنسوبة إليه وفق القانون الجنائي الأمريكي، بينما برأه القاضي الإماراتي من الفعل بسبب أن القوانين الإماراتية وقتها لا تجرم مثل هذا الفعل[1].

ويتضح لنا من خلال المثال السابق خطورة الأثر المترتب على الفراغ التشريعي في مجال مكافحة الجرائم المعلوماتية، والمتمثل في إفلات مرتكبي هذه الجرائم من العقاب على الرغم مما يتسببون فيه من أضرار وخسائر

(1) أشار إلى ذلك د. عمر أبوالفتوح عبدالعظيم الحمامي - مرجع سابق - صـ 336-337

ضخمة، وهو ما يشكل حافزاً لهم على استغلال هـذا الفـراغ لارتكـاب المزيـد مـن هـذه الجرائم .

وسنركز في هذا المطلب عـلى أبـرز الجهـود التشـريعية الدوليـة والإقليميـة لحمايـة سـرية المعلومـات الإلكترونيـة ومكافحـة الجـرائم الماسـة بهـا باعتبارهـا موضـوع هـذا البحث.

الفرع الأول

الجهود التشريعية الدولية لحماية المعلومات الإلكترونية ومواجهة الجرائم الماسة بسريتها

حرص المجتمع الدولي على توفير الحماية للمعلومات والبيانات بمختلف أنواعها وتبنى في سبيل ذلك عدد من الاتفاقيات والقرارات الدولية أهمها:

أولا: الدليل الإرشادي لحماية الخصوصية ونقل البيانات الخاصة الصادر عن منظمة التعاون الاقتصادي والتنمية Organisation for Economic Co-operation and Development (OECD):

تم إعداد هذا الدليل في عام 1980، وقد تضمن مجموعة من القواعد التي تشكل ضمانة للمعلومات والبيانات الشخصية المعالجة إلكترونياً، في كل مرحلة من مراحل الجمع والتخزين والمعالجة والنشر. وتتلخص هذه مبادئ في مشروعية جمع البيانات، وتحديد الغرض من جمعها واستخدامها للغرض الذي جمعت من أجله، و توفير وسائل حماية أمن المعلومات وضمان سريتها. ويختص نطاق هذه القواعد البيانات والمعلومات المتعلقة بالأشخاص الطبيعيين فقط في القطاعين الحكومي والخاص، وتشمل البيانات المعالجة آليا أو المعدة يدويا[1].

ثانياً: قرار الجمعية العامة للأمم المتحدة 95/45 لسنة 1990 بشأن مبادئ توجيهية لتنظيم ملفات البيانات الشخصية المعدة بالحاسبة الإلكترونية

صدر هذا القرار عن الجمعية العامة للأمم المتحدة بتاريخ 14 ديسمبر 1990، ويتضمن مجموعة من المبادئ التي يجب إدخالها في التشريعات الوطنية، والتي تمثل الحد الأدنى من الضمانات للبيانات الشخصية المعدة بالحاسبة الإلكترونية، ومنها:

---

(1) د. يونس عرب - بعنوان الخصوصية وحماية البيانات - مرجع سابق - صـ 26-27

1. مبدأ المشروعية والنزاهة في جمع المعلومات المتعلقة بالأشخاص أو تجهيزها وعدم استخدامها لأغراض مخالفة لمقاصد ميثاق الأمم المتحدة ومبادئه.

2. مبدأ الصحة والذي بمقتضاه يلتزم المسئولون عن إعداد ملفات البيانات أو المسئولون عن حفظها بالتحقق من دقة البيانات المسجلة وملاءمتها

3. مبدأ تحديد الغاية من إنشاء الملف الذي يتضمن البيانات الشخصية والتي يجب أن تكون محددة ومشروعة ومعلنة قبل إنشائه حتى يتسنى إعمال الرقابة على أن البيانات الشخصية المذكورة لا تستخدم أو تفشى لغايات لا تتفق مع الغايات المحددة دون موافقة الشخص المعني.

4. مبدأ وصول الأشخاص المعنيين إلي الملفات: والذي يقر حق الشخص أيا كانت جنسيته أو محل إقامته، أن يعرف ما إذا كانت تجري معالجة آلية لبيانات تتعلق به، وأن يخطر بذلك بشكل مفهوم، وإجراء عمليات التصويب أو المحو التي يراها بالنسبة للبيانات التي تفتقر إلي المشروعية أو اللزوم أو الدقة.

5. مبدأ الأمن: حيث يتعين تضمين على سلطات الدولة اتخاذ التدابير الملائمة لحماية الملفات سواء ضد المخاطر الطبيعية، مثل فقدها عرضيا أو تلفها، أو المخاطر البشرية مثل الاطلاع عليها بغير إذن أو استخدام البيانات بشكل غير أمين.

6. مبدأ الرقابة والعقوبات: بمقتضى هذا المبدأ يجب أن تحدد كل دولة وفقا لنظامها القانوني الداخلي جهاز متخصص يمتاز بالحياد والكفاءة التقنية لمراقبة مراعاة تطبيق المبادئ الواردة بهذا القرار. كما تلتزم الدول بتضمين تشريعاتها الوطنية عقوبات جنائية ملائمة توقع على كل من يخل بتلك المبادئ

ونلاحظ أن المبادئ السابقة تكاد تكون متطابقة مع القواعد التي تضمنها الدليل الإرشادي لحماية الخصوصية ونقل البيانات الخاصة الصادر عن منظمة التعاون الاقتصادي والتنمية المشار إليها في البند السابق، وتتشابه أيضا معها في نطاق تطبيقها حيث حدد البند (10) من هذا القرار نطاق تطبيق المبادئ التي وردت به على جميع الملفات العامة والخاصة المعالجة آليا، بما في ذلك، الملفات التي تعالج يدويا بشرط إجراء التكييف الملائم، إلا أن هذا القرار في سبيل توسيع نطاق تطبيق جميع المبادئ التي وردت به، أو جزء منها فقد أجاز هذا البند وضع أحكام خاصة، اختياريا لتشمل ملفات الأشخاص المعنويين طالما احتوت في جزء منها على معلومات تتعلق بأشخاص طبيعيين.

ثالثا: اتفاقية الجوانب المتصلة بالتجارة من حقوق الملكية الفكرية (اتفاقية التربس)

تضطلع اتفاقية الجوانب المتصلة بالتجارة من حقوق الملكية الفكرية (التربس) منذ إقرارها في عام 1995 وحتى الآن بدور رئيس في مجال حماية الملكية الفكرية نظراً لتضمنها قواعد تشمل كافة فروع وأقسام الملكية الفكرية، بالإضافة إلى اتفاقيات برن لحماية المصنفات الأدبية والفنية 1971، وباريس لحماية الملكية الصناعية 1967 ، وروما لحماية فناني الأداء ومنتجي التسجيلات الصوتية وهيئات الإذاعة، وواشنطن بشأن الملكية الفكرية فيما يتعلق بالدوائر المتكاملة[1].

ووفقا لأحكام الفقرة الثانية من المادة الأولى من اتفاقية التربس فإن المعلومات السرية "المعلومات غير المفصح عنها" تدخل ضمن مصطلح الملكية الفكرية بالإضافة إلى حقوق المؤلف والحقوق المتعلقة بها , العلامات التجارية , المؤشرات الجغرافية , التصميمات الصناعية , براءات الاختراع ,

---

(1) محمود أحمد عبابنة - جرائم الحاسوب وأبعادها الدولية - دار الثقافة للنشر والتوزيع - الأردن - عمان 2009- صـ 163، والموقع الإلكتروني لمنظمة الويبو http //www.wipo int/treaties/ar,

التصميمات التخطيطية للدوائر المتكاملة [1].

وقد أضفت هذه الاتفاقية بموجب المادة (39) - القسم 7 من الجزء الثاني منها حماية للمعلومات غير المفصح عنها حيث تنص تلك المادة على أنه (1- أثناء ضمان الحماية الفعالة للمنافسة غير المنصفة حسب ما تنص عليه المادة (10) مكررة من معاهدة باريس 1967 ، تلتزم البلدان الأعضاء بحماية المعلومات السرية وفق الفقرة (3). 2- للأشخاص الطبيعيين والاعتباريين حق منع الإفصاح عن المعلومات التي تحت رقابتهم بصورة قانونية لآخرين أو حصولهم عليها أو استخدامهم لها دون الحصول على موافقة منهم ، بأسلوب يخالف الممارسات التجارية النزيهة طالما كانت تلك المعلومات :

أ) سرية من حيث أنها ليست ، بمجموعها أو في الشكل والجميع الدقيقين لمكوناتها معروفة عادة أو سهلة الحصول عليها من قبل أشخاص في أوساط المتعاملين عادة في النوع المعنى من المعلومات؛

ب) ذات قيمة تجارية نظرا لكونها سرية ؛

ج) أخضعت لإجراءات معقولة في إطار الأوضاع الراهنة من قبل الشخص الذي يقوم بالرقابة عليها من الناحية القانونية بغية الحفاظ على سريتها.)[2]

وبناء على المادة السابقة فإن المعلومات غير المفصح عنها محل الحماية تشمل:

- المعلومات السرية التي تخص الأشخاص الطبيعيين والاعتباريين وتقع تحت سيطرتهم ورقابتهم بصورة قانونية.

---

(1) نص الاتفاقية منشور على الموقع الإلكتروني http://www.gccpo.org/conve/Trips.pdf

(2) نص الاتفاقية منشور على الموقع الإلكتروني http //www.gccpo org/conve/Trips.pdf

- بيانات الاختبارات أو البيانات الأخرى غير المفصح عنها التي يتم تقديمها إلى الجهات الحكومية كشرط للحصول على الموافقة على تسويق الأدوية أو المنتجات الكيماوية الزراعية التي تستخدم مواد كيميائية جديدة.

وتطبق الحماية على المعلومة التي لها صفة السرية، والتي تستمد قيمتها التجارية من كونها سرية وأنها أخضعت لإجراءات معقولة بغية الحفاظ على سريتها.

ويلاحظ أن الاتفاقية لا تقضى بأن تعامل المعلومات غير المفصح عنها على أنها شكل من أشكال الملكية، ولكنها تنص على تمكين الأشخاص الاعتباريين أو الطبيعيين من منع الإفصاح عن هذه المعلومات التي تحت رقابتهم بصورة قانونية للآخرين، أو حصولهم عليها أو استخدامهم لها دون الحصول على موافقة من أصحابها، وذلك بطريقة منافية للممارسات التجارية الشريفة[1]. والطريقة المنافية للممارسات التجارية النزيهة تشمل مخالفة العقود، وخيانة الثقة أو الإغواء بالمخالفة، وكذلك الحصول على المعلومات غير المفصح عنها بواسطة أطراف ثالثة كانوا على علم بها.أو ساهموا عن غير قصد في إفشاء هذه المعلومات.

وباستعراض أبرز الجهود التشريعية على المستوى الدولي لحماية سرية المعلومات، نرى أنه بات من الضروري صياغة اتفاقية دولية ملزمة لكافة الدول لمكافحة الجرائم المعلوماتية، وأساس هذا الإلزام أن التكنولوجيا جعلت من العالم قرية واحدة صغيرة، وبالتالي فإنه لابد من وجود قانون عام يحكم هذه (القرية الصغيرة)، يتضمن نماذج للأفعال المجرمة، وتحديد سبل التعاون بين الدول في مجال مكافحة تلك الجرائم، وذلك كله بغية التغلب على الفروقات التشريعية بين الدول أو الفراغ التشريعي في بعض الدول،

---

(1) د.حسام الدين الصغير - ورقة عمل مقدمة بالاجتماع المشترك بين الويبو وجامعة الدول العربية حول الملكية الفكرية لممثلي الصحافة والإعلام - القاهرة، 23 و 24 مايو/ أيار 2005 - رمز المستند -WIPO LAS/IP/JOURN/CAI/05/2 – ص 9

وهو ما يشكل ثغرات يستغلها مرتكبي هذه الجرائم للإفلات من العقاب.

ومن جانبي أقترح تبني اتفاقية بودابست المتعلقة بالجرائم الإلكترونية الصادرة عن المجلس الأوروبي والموقعة في 23 نوفمبر 2001، من قبل الأمم المتحدة وطرحها كمشروع اتفاقية دولية لمكافحة الجرائم المعلوماتية نظراً لشمولها على الجوانب الموضوعية والإجرائية للجرائم المعلوماتية فضلاً عن تغطيتها لمجالات التعاون الدولي لمكافحتها وهو ما جعلها أبرز الاتفاقيات متعددة الأطراف في هذا المجال ونموذج تحتذي مختلف الدول عند صياغة تشريعاتها الوطنية الخاصة بجرائم المعلومات، أضف إلى ما تقدم، فأن تلك الاتفاقية تلقى قبول واستحسان دوليين، ويتجلى ذلك من قيام عدد من الدول من خارج أوروبا بالانضمام إليها، ومن أبرزها الولايات المتحدة الأمريكية واليابان وكندا وجنوب أفريقيا.

الفرع الثاني

الجهود التشريعية الإقليمية لحماية المعلومات الإلكترونية ومواجهة الجرائم الماسة بسريتها

نستعرض في هذا الفرع أبرز الجهود التشريعية الإقليمية على المستوى الأوروبي لانطوائها على جهود هامة في مجال حماية المعلومات، والتي شكلت نموذجاً لكثير من دول العالم في هذا المجال. ثم ننتقل لنلقي الضوء على الجزء الذي يهمنا كمنطقة عربية واستعراض ابرز الجهود على المستوى العربي في هذا المجال أيضا، للوقوف على مدى كفايتها وفاعليتها.

أولا: على المستوى الأوروبي:

كان للدول الأوروبية والغربية منها تحديداً السبق في مجال التشريعات الخاصة بالجرائم المعلوماتية وحماية البيانات والمعلومات المعالجة آليا، وذلك بحكم كونها أحد منابع ثورة المعلومات التي انطلقت إلى باقي دول العالم، وأولى الدول التي غاصت في بحور تقنيات المعلومات والاعتماد عليها بشكل كبير، وأولى الدول التي انكوت بنار تلك التقنية، وأمام مخاطر وتحديات تلك التقنية الحديثة، كان لزاما على تلك الدول أن تتخذ من التشريعات درعاً واقيا لها ولمؤسساتها وأفرادها لصد تلك المخاطر. ومن أبرز تلك الجهود التشريع ما يأتي:

1- اتفاقية المجلس الأوروبي بشأن حماية الأفراد في مواجهة المعالجة الآلية للبيانات الشخصية 1981:

لقد أبرمت هذه الاتفاقية في 28 يناير 1981 بمدينة ستراسبورغ، بفرنسا وأصبحت نافذة بتاريخ 1985/10/1، وهذه الاتفاقية ملزمة للدول المصدقة عليها، وتتضمن المبادئ التي تمثل الحد الأدنى لمعايير حماية الخصوصية المتعين على الدول الأطراف تضمينها في التدابير التشريعية

والقوانين التي تضعها[1]، وهذه المبادئ تتقارب لحد كبير مع مبادئ منظمة التعاون الاقتصادي والتنمية ، والمبادئ التي تضمنها قرار الجمعية العامة للأمم المتحدة 95/45 لسنة 1990 بشأن مبادئ توجيهية لتنظيم ملفات البيانات الشخصية المعدة بالحاسبة الإلكترونية، السالف بيانهما.

وقد طلب البرلمان الأوروبي من الاتحاد الأوروبي دفع الدول الأعضاء إلى توقيع على هذه الاتفاقية، والذي بدوره أصدر بتاريخ 1981/7/29 توصية للدول الأعضاء بالتوقيع عليها. ويضاف إلى الجهود السابقة على المستوى الأوربي سبق إصدار الاتحاد الأوروبي مجموعة من التعليمات المتعلقة بخصوص حماية بيانات الأفراد مثل تعليمات 76/4/8 المتعلقة بحماية الأفراد من أنشطة التقييم الآلي للبيانات، وتعليمات 79/5/8 المتعلقة بحماية الأفراد في مواجهة التطور التقني لمعالجة البيانات، وتعليمات 82/3/9 بذات الموضوع [2]. وقد كان انعكست تلك الجهود على التشريعات الوطنية للدول الأوروبية مثل فرنسا والتي أصدرت بتاريخ 6 يناير 1978 القانون رقم 17- 78 الخاص بحماية البيانات الاسمية للمواطنين في مواجهة نظم لمعالجة الآلية للمعلومات[3]، وقانون حماية البيانات الانجليزي الصادر بتاريخ 16 يوليو 1998[4].

2-اتفاقية المجلس الأوروبي بشأن مكافحة الجرائم المعلوماتية الموقعة في 23 نوفمبر 2001 – بمدينة بودابست – المجر.

سبق وأن تناولنا أحكام هذه الاتفاقية في مواقع سابقة من هذا البحث، إلا أنه كان لزاماً أن نتعرض إليها ولو بشكلٍ موجز في معرض الحديث عن الجهود التشريعية الإقليمية لحماية سرية المعلومات الإلكترونية ومكافحة الجرائم الماسة بها، باعتبارها أبرز تلك الجهود وأكثرها ارتباطاً بالجريمة

---

(1) نص الاتفاقية منشور على موقع الإلكتروني للجنة الاقتصادية والاجتماعية لغربي آسيا (الإسكوا) http://isper.escwa.un.org

(2) د. يونس عرب – بحث بعنوان الخصوصية وحماية البيانات – مرجع سابق – صـ 29-30

(3) د. عمر أبوالفتوح عبدالعظيم الحمامي – مرجع سابق – صـ 288

(4) نص القانون منشور على موقع الإلكتروني http://www.legislation.gov.uk/ukpga

المعلوماتية.

أقدمت الدول الأعضاء في المجلس الأوروبي والدول الآخرى الموقعة على هذه الاتفاقية، على هذه الخطوة وفقا لما جاء في ديباجة هذه الاتفاقية، إدراكاً منها بالحاجة لإيجاد سياسة جنائية مشتركة، تهدف إلى حماية المجتمع من جرائم الفضاء المعلوماتي واعترافاً منهم بالحاجة للتعاون المتبادل بين الدول والقطاع الصناعي الخاص في محاربة جرائم الفضاء المعلوماتي إيماناً منهم بأن المكافحة الفعالة لجرائم الفضاء المعلوماتي تستلزم مزيد من التعاون الدولي السريع و الفعال في المسائل الجنائية [1].

جسدت اتفاقية بودابست لمكافحة الجرائم المعلوماتية الجهود التي بذلها المجلس الأوروبي للتصدي لهذا النوع من الجرائم التي شكلت تحديا خطيراً وتهديداً حقيقياً لمصالح للدول والأفراد والمؤسسات.

وقد ضمت هذه الاتفاقية معظم الدول الأوروبية بالإضافة إلى كندا، واليابان، وجنوب أفريقيا، والولايات المتحدة وطرحت للتوقيع في بودابست - المجر في تاريخ 23 نوفمبر 2001ودخلت حيز التنفيذ في الأول من يوليو 2004 ويمكن لأية دولة في العالم الانضمام للاتفاقية إذا ما رغبت بذلك [2].

وتتألف هذه الاتفاقية من 48 مادة وتغطي الاتفاقية مجموعة كبيرة من الجرائم الجنائية، على النحو الأتي:

- الجرائم ضد سرية وسلامة وإتاحة البيانات والنظم (المواد من 2-6): وتشمل جرائم الولوج غير القانوني، الاعتراض غير القانوني، الاعتداء على سلامة البيانات، الاعتداء على سلامة النظام، إساءة استخدام

---

(1) هذه الاتفاقية منشورة باللغة العربية على الموقع الإلكتروني للملجس الأوروبي وهو :

http://www coe int/t/DGHL/cooperation/economiccrime/cybercrime/default_en.asp

(2) كريستينا سكولمان- مرجع سابق- صـ40.

أجهزة الحاسب.

- الجرائم المتصلة بالحاسب (المواد من 7- 8): وتشمل التزوير المعلوماتي، والغش المعلوماتي.

- الجرائم المتصلة بالمحتوى (المادة 9): وهي الجرائم المتصلة بالمواد الإباحية الطفولية عبر النظم المعلوماتية.

- الجرائم المتصلة بالانتهاكات الخاصة بحقوق الملكية الفكرية والحقوق المجاورة لها. (المادة 10)

- الشروع والاشتراك في الجرائم المعلوماتية (المادة 11).

وأوجبت هذه الاتفاقية أيضاً تقرير مسئولية الأشخاص المعنوية وذلك بموجب المادة (12).

ولم تقتصر اتفاقية بودابست على جوانب الحماية الجنائية الموضوعية فحسب، بل شملت كذلك الجوانب الإجرائية وذلك بالمواد من (14 – 22) وتشمل: نطاق تطبيق الإجراءات الجنائية وشروطها وضماناتها، والتحفظ العاجل على البيانات المعلوماتية المخزنة، الأمر بإنتاج أو تقديم بيانات معلوماتية، تفتيش وضبط البيانات المعلوماتية المخزنة، والاختصاص القضائي.

فيما نظمت موضوع التعاون الدولي وهو أحد الأهداف الأساسية للاتفاقية بالمواد من (23-34)، وتشمل ؛ المبادئ العامة المتعلقة بالتعاون الدولي، والمبادئ المتعلقة بتسليم المجرمين، والمساعدة القضائية المتبادلة، والإجراءات المتعلقة بالمساعدة المتبادلة في حالة عدم وجود اتفاقيات دولية واجبة التطبيق.

وعلى النحو المتقدم تكون اتفاقية بودابست 2001نموذجاً وركيزة أساسية، في مجال مكافحة الجرائم المعلوماتية، تسترشد باقي دول العالم في صياغة تشريعاتها الوطنية أو لإبرام اتفاقيات ثنائية أو إقليمية أو دولية.

ثانياً : على المستوى العربي:

وفقا لتقرير مؤتمر الأمم المتحدة الثاني عشر لمنع الجريمة والعدالة الجنائية الذي عقد في مدينة سلفادور، البرازيل في الفترة من 12 إلى ١٩ أبريل ٢٠١٠، تعد الدول النامية بما فيها الدول العربية من أكثر الدول عرضة لمخاطر الجرائم المعلوماتية [1]. مما يجعلها بحاجة إلى وضع آليات تشريعية محددة لمكافحة تلك الجرائم، وقد عملت الدول العربية من خلال جامعة الدول العربية على توحيد جهودها التشريعية في سبيل مكافحة الجريمة بشكل عام والجرائم المعلوماتية بما فيها الجرائم الماسة بسرية المعلومات الإلكترونية بشكل خاص وهي جهود حميدة،وفيما يلي نستعرض أبرز تلك الجهود.

1- القانون الجزائي العربي الموحد الاسترشادي:

اعتمد مجلس وزراء العدل العرب بتاريخ 19 نوفمبر 1996 القانون الجزائي العربي الموحد كقانون نموذجي وذلك بالقرار رقم 229- د 12[2]. وقد جرم هذا القانون الاعتداء على حقوق الأشخاص الناتج عن الجذاذات والمعالجات المعلوماتية، وذلك بالمواد (461 – 464)، حيث جرمت المواد من 461 – 463 جمع المعلومات الاسمية أو معالجتها آليا، أو استعمالها بالمخالفة لأحكام القانون، أو المساس بسلامة وسرية معلومات الأشخاص

وبمطالعة المادتين 462، 464، نلاحظ أنهما تناولتا صورتين من صور الجرائم الماسة بسرية المعلومات الإلكترونية، حيث تناولت المادة 462 جريمة الاعتراض غير القانوني للبيانات والمعلومات الشخصية للأفراد الطبيعيين فقط، حيث تنص تلك المادة على أنه (يعاقب بالحبس مدة لا تزيد على سنة وبالغرامة كل من حصل على معلومات أسمية خاصة بالغير، أثناء

---

(1) تقرير مؤتمر الأمم المتحدة الثاني عشر لمنع الجريمة والعدالة الجنائية سلفادور، البرازيل في الفترة من 12 إلى 19 أبريل 2010 – رمز الوثيقة A/CONF.213 - ص 71

(2) هذا القانون منشورعلى الموقع الإلكتروني لجامعة الدول العربية http://www.arableagueonline.org

تسجيلها أو ترتيبها أو إرسالها بأية وسيلة من وسائل المعالجة التي من شأن إفشائها المس بسمعة المعنى بالأمر أو بحياته الشخصية، مما يمكن إطلاع الغير ممن لا تسمح له صفته الاطلاع على تلك المعلومات دون إذن المعنى بالأمر).

في حين تناولت الفقرة الأولى من المادة 464 جريمة الدخول غير المصرح به أو البقاء داخل نظام المعالجة الآلية حيث تنص على أنه (يعاقب بالحبس والغرامة أو بإحدى هاتين العقوبتين كل من : 1- دخل بطريق الغش إلى كامل أو جزء من نظام المعالجة الآلية للمعلومات، أو بقي فيه، وتضاعف العقوبات إذا نتج عن ذلك إما محو المعلومات التي يحتوى عليها النظام أو تعديلها ، ...). وهو ما يقابل نص المادة 2/462 من القانون الفرنسي الصادر في 1988 بشأن جرائم الغش المعلوماتي والتي يقابلها المادة 1/323 من قانون العقوبات الفرنسي الجديد رقم 1336 لسنة 1992، السابق تناولهما في الجزئية الخاصة بجريمة الدخول غير القانوني أو البقاء داخل النظام المعلوماتي في هذا البحث.

2- قانون الإمارات العربي الاسترشادي لمكافحة جرائم تقنية المعلومات وما في حكمها:

جاء هذا القانون كخطوة متقدمة في مجال العمل العربي المشترك لمكافحة الجرائم المعلوماتية، حيث تم اعتماده من قبل كل من مجلس وزراء العدل العرب في دورته التاسعة عشرة بالقرار رقم 495 – د 19 – 2003/10/8، ومجلس وزراء الداخلية العرب في دورته الحادية والعشرين بالقرار رقم 417 – د 21 / 2004[1]. ويتألف هذا القانون من 27 مادة ، تشمل صور الجرائم المعلوماتية المختلفة، بما فيها جرائم الدخول غير المصرح به أو البقاء داخل النظام المعلوماتي (المادة 3)، والاعتراض أو

---

(1) نص هذا القانون منشور على الموقع الإلكتروني لجامعة الدول العربية http://www.arableagueonline.org

الالتقاط غير القانوني للمعلومات والبيانات (المادة 8)، بالإضافة إلى الجرائم المعلوماتية الآخرى مثل إعاقة النظام و إتلاف البيانات والمعلومات و الاحتيال والتزوير وغيرها.

وقد تم إعداد هذا القانون ليكون بمثابة نموذج أو دليل تسترشد به كل دولة عضو بالجامعة العربية عند سنها تشريعاً وطنياً خاص بمكافحة الجرائم المعلوماتية.

ويعد ذلك في تقديري مثال هام على التعاون الإقليمي والدولي لمكافحة الجرائم المعلوماتية، كونه يشكل نوعاً من المساعدة للدول التي تفتقر إلى الخبرات والكفاءات في هذا المجال لتطوير بنيتها التشريعية، فضلا عما يشكله من فرصة لتبادل الأفكار في هذا المجال، فالصورة الإجرامية التي قد تظهر في دولة ما قد لا تظهر في ذات الوقت في دولة آخرى، وبهذا تكون مثل هذه القوانين فرصة لسد الثغرات التي قد ينفذ من خلالها مجرمي المعلوماتية.لذا نرى، أنه ونظراً لقيام الدول العربية بإبرام اتفاقية خاصة بمكافحة جرائم تقنية المعلومات في عام 2010 والتي سنتناولها فيما يلي، فأنه يتعين إعادة طرح هذا القانون النموذجي للمناقشة من قبل الجهات المختصة بالجامعة العربية مثل مجلسي وزراء العدل والداخلية العرب، لإعادة النظر فيه وإجراء التعديلات اللازمة عليه في ضوء تلك الاتفاقية. ونقترح أن يكون هذا القانون النموذجي حاضراً بشكل دوري على طاولة اجتماعات المختصين بالدول العربية لمراجعته بشكل مستمر وإدخال التعديلات اللازمة عليه بما يجعله نموذجاً متطوراً بقدر التطور السريع الذي تتسم به هذه الجرائم المعلوماتية.

3- الاتفاقية العربية لمكافحة جرائم تقنية المعلومات 2010.

أبرمت هذه الاتفاقية في 21/ 12/ 2010 ووقع عليها سبع عشرة دولة

عربية[1]. وقد عبرت المادة الأولى منها عن الهدف الذي تنشده وهو تعزيز التعاون فيما بين الدول العربية لمكافحة جرائم تقنية المعلومات التي تهدد أمنها ومصالحها وسلامة مجتمعاتها، وذلك بتبني سياسة جنائية مشتركة تهدف إلى حماية أمن المجتمع العربي وأفراده ومصالحهم ضد تهديدات جرائم تقنية المعلومات.وقد جاءت هذه الاتفاقية بعد مطالبات عدة من قبل المختصين في أكثر من مناسبة بإصدار مثل هذه الاتفاقية، حيث تضمن "إعلان القاهرة لمكافحة الجريمة الإلكترونية 2007 " الصادر عن المؤتمر الإقليمي الأول حول الجريمة الإلكترونية المنعقد في القاهرة بتاريخ 26-27 نوفمبر 2007، دعوة الدول العربية إلى الإسراع في إقرار تشريعات لمكافحة الجرائم الإلكترونية، وتشجيع الدول المنطقة العربية للاسترشاد باتفاقية بودابست بشأن الجرائم المعلوماتية 2001 عند إعداد القوانين الموضوعية والإجرائية الخاصة بمكافحة الجرائم المعلوماتية [2]

وتتألف هذه الاتفاقية من 43 مادة ، شملت الجوانب الموضوعية والإجرائية الخاصة بالجرائم المعلوماتية، ومظاهر التعاون بين الدول الأعضاء. حيث تضمن الفصل الثاني بالمواد (6 - 18) صور الأفعال التي جرمتها الاتفاقية وهي (الدخول غير المشروع، والاعتراض غير المشروع، الاعتداء على سلامة البيانات، إساءة استخدام وسائل تقنية المعلومات، التزوير، الاحتيال، الإباحية، الجرائم المرتبطة بالإباحية -المقامرة والاستغلال الجنسي- ، الاعتداء على حرمة الحياة الخاصة، الجرائم المتعلقة بالإرهاب والمرتكبة بواسطة تقنية المعلومات، الجرائم المتعلقة بالجرائم المنظمة والمرتكبة بواسطة تقنية المعلومات، الجرائم المتعلقة بانتهاك حق المؤلف والحقوق المجاورة، الاستخدام غير المشروع لأدوات الدفع لالكترونية). وتناولت المادة (19) أحكام الشروع والاشتراك في ارتكاب

---

(1) نص هذا الاتفاقية منشورة على الموقع الإلكتروني لجامعة الدول العربية

http://www.arableagueonline.org

(2) الموقع العربي للملكية الفكرية http //www.arabipcenter com/public/CyberCrimeLaws

الجرائم السابقة، أما المادة (20) فنصت على المسئولية الجنائية للأشخاص الطبيعية والمعنوية. وقد تم تخصيص الفصل الثالث من الاتفاقية للأحكام الإجرائية وذلك بالمواد (22 - 29) وتلك الأحكام هي (نطاق تطبيق الأحكام الإجرائية، التحفظ العاجل على البيانات المخزنة في تقنية المعلومات، التحفظ العاجل والكشف الجزئي لمعلومات تتبع المستخدمين،أمر تسليم المعلومات، تفتيش المعلومات المخزنة، ضبط المعلومات المخزنة، الجمع الفوري لمعلومات تتبع المستخدمين، اعتراض معلومات المحتوى).

في حين خصص الفصل الرابع للتعاون القانوني والقضائي بالمواد (30 - 42) وصور هذا التعاون هي (تسليم المجرمين، المساعدة المتبادلة، المعلومات العرضية المتلقاة، الإجراءات المتعلقة بطلبات التعاون والمساعدة المتبادلة، وحالات رفض المساعدة، الحفظ العاجل للمعلومات المخزنة على أنظمة المعلومات، الكشف العاجل لمعلومات تتبع المستخدمين المحفوظة، التعاون والمساعدة الثنائية المتعلقة بالوصول إلى معلومات تقنية المعلومات المخزنة، الوصول إلى معلومات تقنية المعلومات عبر الحدود، التعاون والمساعدة الثنائية بخصوص الجمع الفوري لمعلومات تتبع المستخدمين، التعاون والمساعدة الثنائية فيما يخص المعلومات المتعلقة بالمحتوى)

وبنظرة عامة على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات،يلاحظ أنها شملت كافة المسائل اللازمة لمكافحة الجرائم المعلوماتية بشكل عام ، من حيث الصور الإجرامية، ومجالات التعاون القانوني والقضائي التي تتناسب وطبيعة الجرائم المعلوماتية من سرعة في جمع الأدلة وملاحقة المجرمين، وهو ما يكسبها قيمة وفاعلية في مجال مكافحة تلك الجرائم.ومن زاويا آخرى فإن هذه الاتفاقية نظراً لإلزامية نصوصها لكافة الدول الموقعة عليها، فإنها تعد بمثابة حافز للدول التي مازالت تعاني فراغ أو قصور تشريعي أن تعالجه، تنفيذا لالتزامها بهذه الاتفاقية.

وبالإضـافة إلى مـا تقـدم يلاحـظ تـأثر هـذه الاتفاقيـة،بنظيرتها الأوربيـة - اتفاقيـة بودابسـت الخاصـة بـالجرائم المعلوماتيـة 2001- بـل تكـاد تتطـابق معهـا في معظـم نصوصها، لذا نقترح أنه طالما تلـك الاتفاقيـة تحمـل ذات المبـادئ المقبولـة لـدى الـدول العربية، قيام الدول العربية بالانضمام إلى تلك الاتفاقية لما في ذلك من فائدة كبـيرة لهـا خاصة على صعيد مجالات التعاون الدولي، من تسليم وملاحقة المجـرمين وجمـع الأدلـة وغيرها، بما يمكن الدول العربية من التصدي للكم الهائـل مـن الهجـمات الإلكترونيـة أو المعلوماتية التي في الغالب ما يكون مصدره الولايات المتحدة الأمريكية وأوروبا.

المطلب الثاني

الجهود التشريعية الوطنية لحماية المعلومات الإلكترونية ومواجهة الجرائم الماسة بسريتها

أكدت مختلف دول العالم في أكثر من مناسبة على أهمية التشريعات الوطنية كشرط أساسي لازم في مجال مكافحة الجرائم المعلوماتية[1] ، فالفراغ التشريعي في دولة ما قد يجعل منها ملاذا آمنا لمرتكبي هذه الجرائم، مثال ذلك، فقد قام أحد مجرمي المعلومات فلبيني الجنسية بصنع فيروس يسمى (أحبك) (I Love You) تسبب في خسائر قدرت بحوالي (7) مليارات دولار، وتمكن من الإفلات من العقاب وتم الافراج عنه، حيث أسقطت التهم الموجهة إليه من جانب السلطات الفليبينية وذلك لعدم تجريم القانون الفلبيني هذه الأفعال في تلك الفترة[2].لذا فقد أقدمت مختلف الدول إلى اتخاذ تدابير تشريعية لمواجهة المخاطر والتهديدات المتزايدة الناجمة عن إساءة استعمال تكنولوجيا المعلومات، وذلك بسن تشريعات خاصة، أو إجراء تعديلات على قوانين العقوبات القائمة لديها، على النحو الذي يكفل للمجتمعاتها الحماية اللازمة من هذه الأخطار، والتي من بينها الأفعال الماسة بسرية المعلومات والبيانات الإلكترونية، حيث أكد قرار الجمعية العامة الأمم المتحدة رقم (A/55/63 الصادر 4 ديسمبر 2000 بدورتها الخامسة والخمسون على أنه (ينبغي للنظم القانونية أن تحمي سرية البيانات ونظم الحواسيب وسلامتها وتوافرها، من أي عرقلة غير مأذون بها، وأن تضمن معاقبة من يقوم بإساءة استعمالها لأغراض إجرامية)[3].

---

(1) مؤتمر الأمم المتحدة الحادي عشر لمنع الجريمة والعدالة الجنائية – ورقة عمل بعنوان تدابير لمكافحة الجرائم المتصلة بالحواسيب- مرجع سابق – صـ 18، و تقرير مؤتمر الأمم المتحدة الحادي عشر لمنع الجريمة والعدالة الجنائية -بانكوك 2005 – رمز الوثيقة A/CONF.203/ 18

(2) جان فرنسوا هنروت – مرجع سابق- صـ 95-97.

(3)http://www.un.org/arabic/documents/GARes/55/A_RES_55_063.pdf

وفي ضوء ما سبق سنتناول في هذا المطلب أبرز الجهود التشـريعة عـلى المسـتوى الوطني لحمايـة سـرية المعلومـات الإلكترونيـة في بعـض دول المنتميـة إلى المجموعـة اللاتينية والأنجلوأمريكة، كما سنتناول أبرز الجهود التشـرية في بعض الـدول العربيـة، وذلك على النحو الآتي:

الفرع الأول

الجهود التشريعة الوطنية لحماية المعلومات الإلكترونية ومواجهة الجرائم الماسة بسريتها في بعض دول المجموعة اللاتينية والأنجلوأمريكة

استجابة دول أوروبا الغربية والولايات المتحدة الأمريكية سريعاً لمتطلبات عصر تقنية المعلومات، واتخذت التدابير التشريعة اللازمة التي تمكنها من صد الآثار السلبية الإجرامية الناجمة عن إساءة استعمال هذه التقنية، وسنبرز من خلال هذا الجزء من البحث أهم تلك الجهود بغية الاستفادة من تجاربهم في هذا المجال، والتعرف على موقعنا كدول عربية، ومملكة البحرين على وجه الخصوص في مجال حماية سرية المعلومات الإلكترونية، بالمقارنةً بتلك الدول، من حيث ما إذا كنا متأخرين عنها من عدمه.

أولا: دول المجموعة اللاتينية:

المجموعة اللاتينية هي؛ التي تنتمي أصولها إلى القانون الروماني، ومن أبرز تطبيقاتها القانون الفرنسي والقوانين التي استمدت منه قواعده.

1- فرنسا: أقرت فرنسا عدة قوانين المتعلقة لحماية المعلومات ومكافحة الجرائم الماسة بسريتها، أبرزها:

أ- القانون رقم 17 لسنة 1978، الخاص بحماية البيانات الإسمية للمواطنين في مواجهة نظم المعالجة الآلية, والذي صدر لضمان حماية سرية حياة الأفراد، ومن بين الجرائم التي تضمنها هذا القانون، جريمة التسجيل أو الحفظ غير المشروع للبيانات الإسمية، وجريمة الإفشاء غير المشروع للبيانات الأسمية.[1]

ب- القانون رقم 19 لسنة 1988 بشأن تعديل قانون العقوبات

---

(1) د.عمر أبوالفتوح عبدالعظيم الحمامي - مرجع سابق - صـ 288- 291

الفرنسي بإضافة مواد خاصة بجرائم الغش المعلوماتي 2/462 - إلى 462/ 9، حيث جرمت المادة 2/462 الدخول أو البقاء غير المشروع داخل النظام المعلوماتي. وقد تم تعديل هذا القانون بموجب القانون رقم 1336 لسنة 1992 [1]

وقد سبق تناول تلك المواد بمناسبة مناقشة جريمتي الدخول أو البقاء داخل النظام المعلوماتي غير القانوني، والاعتراض غير القانوني.

2- بلجيكا: أصدرت مجموعة من القوانين بشأن حماية البيانات الشخصية المعالجة آلية قانون تنظيم استخدام أجهزة الحاسوب في المعالجة الإلكترونية للبيانات الشخصية 1979، قانون حماية الحياة الخاصة فيما يتعلق بالتعامل مع المعطيات الشخصية 1992 المعدل عامي 1998 و 2000[2]، و في عام 2000 أجرى البرلمان البلجيكي تعديلاً على قانون العقوبات وتحديدا تعديل المادة (550/ب) لتشمل جرائم الكومبيوتر مثل الاختراق وإتلاف الكومبيوتر[3].

3- وفي ألمانيا: تم تعديل قانون العقوبات بإضافة قسمين الأول بشأن التجسس على البيانات والآخر بشأن إتلاف الكومبيوتر، بالإضافة إلى قانون خاص بحماية المعطيات 1977 عدل جذريا بتاريخ 1990 كما تم تعديله في العام 1994[4].

4- أما اليابان: فقد أصدرت في عام 1988 قانون رقم 95 بشأن حماية المعلومات الشخصية، وفي عام 1999 قانون رقم 128 بشأن حظر الدخول إلى الكومبيوتر[5].

---

(1) المرجع نفسه- صـ 295

(2) د.يونس عرب –الخصوصية وحماية البيانات – مرجع سابق صـ 56

(3) د.أحمد خليفة الملط – الجرائم المعلوماتية – دار الفكر الجامعي – الإسكندرية 2005 – صـ 145

(4) د. يونس عرب – مرجع سابق – صـ 54

(5) المرجع نفسه - صـ 60

ثانياً : دول المجموعة الانجلوأمريكية:

يرجع النظام الانجلوأمريكي أساساً إلى القانون الإنجليزي القديم، حيث قام الإنجليز بنقله إلى أمريكا الشمالية إبان الاحتلال الإنجليزي في القرن السابع، ويقوم هذا النظام على السوابق القضائية في مجال التجريم والعقاب، ومن الدول التي تبنت هذا النظام إنجلترا والولايات المتحدة الأمريكية وأستراليا وأيسلندا وأيرلندا والهند[1].وقد أصدر عدد كبير من دول هذه المجموعة تشريعات خاصة بحماية المعلومات والبيانات ومكافحة الجرائم الماسة بسريتها، وفيما يلي نستعرض أهم جهود بعض تلك الدول :

1- انجلترا: أصدرت في عام 1990 قانون إساءة الكومبيوتر[2] الذي تناول بالتجريم جريمة الدخول غير القانوني، بالإضافة إلى قانون حماية البيانات الصادر في عام 1984.

2- الولايات المتحدة الأمريكية: تعد الولايات المتحدة الأمريكية أولى الدول التي سنت تشريعات مستقلة بشان جرائم الكمبيوتر، وتتميز بامتلاكها ترسانة من التشريعات تغطي الجوانب المختلفة للجرائم المعلوماتية [3]، ومن تلك التشريعات قانون الاحتيال و إساءة استخدام الحاسوب 1984. وقد تناول التشريع الاتحادي القسم (18) الخاص بالجرائم والإجراءات الجنائية المعدل عام 1996، جرمت المادة (1030) التوصل غير المصرح به (الدخول) إلى أحد أنظمة الكمبيوتر الحكومية وكشف المعلومات السرية ، وكشف المعلومات من جهة غير مصرح بها تلقيها، الدخول غير المصرح به إلى أي كمبيوتر والتوصل إلى معلومات غير مسموح الاطلاع عليها، الدخول غير المصرح به إلى اي كمبيوتر ومن ثم

---

(1) د. عمر أبو الفتوح عبدالعظيم الحمامي – مرجع سابق – صـ 315

(2) نص القانون منشور على الموقع الإلكتروني http://www.legislation.gov.uk/ukpga

(3) د. يونس عرب - قراءة في الاتجاهات التشريعية للجرائم الإلكترونية مع بيان موقف الدول العربية وتجربة سلطنة عمان- ورقة عمل مقدمة بورشة عمل " تطوير التشريعات في مجال مكافحة الجرائم الإلكترونية " هيئة تنظيم الاتصالات / مسقط – سلطنة عمان 2-4 ابريل 200

ارتكاب احتيال. إلحاق أضرار جراء الدخول غير المصرح به سواء للنظام أو البرامج أو للمعلومات المخزنة فيه . بالإضافة قانون الخصوصي 1974، وقانون حرية المعلومات 1976[1]

ونلاحظ مما تقدم، إظهار مدى الاهتمام المبكر الذي أولته تلك الدول لحماية المعلومات والبيانات الشخصية من مخاطر إساءة استخدم التكنولوجيا إلى جانب حماية المعلومات الحكومية، و المعلومات الاقتصادية والمالية وغيرها،على خلاف ما عليه الوضع في كثير من دول منطقتنا العربية الذي كما سنرى فيما يلي، أنه يتسم بالبطء من جهة، ومن جهة أخرى التركيز على حماية المعاملات العسكرية و التجارية والاقتصادية الإلكترونية دون إيلاء المعلومات الشخصية للأفراد الحماية اللازمة.

(1) المرجع نفسه – صـ 6، د. عمر أبو الفتوح عبدالعظيم الحمامي- مرجع سابق – صـ 326-328

الفرع الثاني

الجهود التشريعية الوطنية لحماية المعلومات الإلكترونية ومواجهة الجرائم الماسة بسريتها في بعض الدول العربية

أظهرت دراسة بعنوان (مشروع تنسيق التشريعات السيبرانية لتحفيز مجتمع المعرفة في العالم العربي) قدمت خلال اجتماع خبراء حول البيئة التمكينية لتطوير الخدمات الإلكترونية في المنطقة العربية (مارس 2011)- الأمم المتحدة اللجنة الاقتصادية والاجتماعية لغربي أسيا (الإسكوا) [1] ، أن معظم الدول العربية لديها نقص أو تفتقر لوجود تشريعات متكاملة للفضاء السيبراني، حيث أنه وفقا للمعاهدات والاتفاقات الدولية ذات الصلة، فإن هناك خمسة مواضيع رئيسية يجب تنظيمها قانونا وهي ؛ حماية البيانات الشخصية ومعالجتها، بما في ذلك حق الخصوصية، التجارة الإلكترونية، المعاملات الإلكترونية مثل العمليات المصرفية الإلكترونية والدفع الإلكتروني، جرائم الفضاء السيبراني، والملكية الفكرية [2]. كما تعاني معظم دول المنطقة العربية من بطء في إجراءات إصدار القوانين الخاصة بالفضاء المعلوماتي، ويمكن إرجاع ذلك إلى تعدد الجهات المعنية بذلك مثل وزارات العدل والاتصالات والتجارة والداخلية.

وفي دراسة آخرى أجراها استشاري اللجنة الاقتصادية والاجتماعية لغربي آسيا (الإسكو) عام 2007، أكد أن دول المنطقة العربية ما زالت تعاني من غياب للقوانين المناسبة لحماية معالجة البيانات والحق بالخصوصية. وأنه على الرغم من أن قوانين الوطنية بتلك الدول تنص على بعض المواد، فإن هذه المواد تتعلق في الغالب بالأحوال الشخصية، أو بالإحصاءات أو

---

(1) ميرنا الحاج بربر- الدراسة منشورة على الموقع الإلكتروني css.escwa.org.lb/ICTD/1429/Day2/2.pdf، وجدير بالذكر أن ذات الملاحظات وردت بتقرير مؤتمر المتابعة الإقليمية لمقررات القمة العالمية لمجتمع المعلومات 16-18 يونيو 2009 - دمشق - الأمم المتحدة - المجلس الاقتصادي والاجتماعي - اللجنة الاقتصادية والاجتماعية لغربي آسيا (الإسكوا)- ، رمز الوثيقة E/ESCWA/ICTD/2009/13 – ص 12

(2) سيم حرب (استشاري الإسكوا) دراسة معتمدة من قبل اللجنة الاقتصادية والاجتماعية لغربي آسيا (الإسكو) بالوثيقة رقم - E/ESCWA/ICTD/2007/8 بيروت.- ص3.

بتخزين المعلومات المصرفية. وأنه ما زال هناك نقص في تشريعات حماية البيانات الشخصية في هذه الدول[1]

وبعد استعراض ما تقدم، فإنه بمطالعة الوضع العام في المنطقة العربية نلاحظ أن هناك حراك تشريعي في عدد من الدول العربية نحو استكمال بنيتها التشريعية وسد ما بها من نقص لمكافحة الجرائم المعلوماتية وحماية المعلومات ومن أبرز تلك الجهود ما يأتي:

1- سلطنة عمان: تُعد عمان أولى دول الخليج في تبني قواعد قانونية تجرم الأفعال الإجرامية الناجمة عن إساءة استعمال تقنية المعلومات، وقد بذلت عدة جهود تشريعية في سبيل توفير الحماية لسرية المعلومات الإلكترونية ومن أبرز تلك الجهود ما يأتي:

- المرسوم السلطاني رقم 72 / 2001 بتعديل قانون الجزاء العماني بإضافة فصل ثاني مكرر للباب السابع بالمواد رقم (276) مكرر - (276) مكرر(4) واشتملت المادة (276) مكررا على أحكام هامة لحماية سرية المعلومات الإلكترونية ، حيث جرمت أفعال الالتقاط غير المشروع للمعلومات أو البيانات ،الدخول غير المشروع على أنظمة الحاسب الآلي، التجسس والتصنت على البيانات و المعلومات، انتهاك خصوصيات الغير أو التعدي على حقهم في الاحتفاظ بأسرارهم، جمع المعلومات و البيانات و إعادة استخدامها، تسريب المعلومات والبيانات، نشر واستخدام برامج الحاسب الآلي بما يشكل انتهاكا لقوانين حقوق الملكية و الأسرار التجارية.

ولم يقتصر الأمر على ذلك بل نصت المادة (276) مكرراً (1) معاقبة كل من استولى أو حصل على نحو غير مشروع على بيانات تخص الغير تكون منقولة أو مختزنة أو معالجة بواسطة أنظمة المعالجة المبرمجة للبيانات.

وفي تقديري فأن النصين المتقدمين بصياغتهما العامة كفيلين بحماية سرية

---

(1) المرجع نفسه – صـ 19

المعلومات الإلكترونية بمختلف أشكالها ونؤكد على الشخصية منها.

- المرسوم السلطاني رقم 12 لسنة 2011 بإصدار قانون لمكافحة جرائم تقنية المعلومات[1]: في خطوة تعكس حرص المشرع العُماني وإصراره على مكافحة الجرائم المعلوماتية فقد قام بإلغاء المرسوم بقانون السابق، وأصدر هذا القانون كتشريع خاص بالجرائم المعلوماتية، ويتألف القانون الجديد من (35) مادة ، ويتناول في الفصل الثاني منه جرائم التعدي على سلامة وسرية وتوافر البيانات والمعلومات الإلكترونية والنظم المعلوماتية (المواد من 3- 10)، حيث جرمت المادة (3) الدخول العمدي ودون وجه حق موقعا إلكترونيا أو نظاما معلوماتيا أو وسائل تقنية المعلومات أو جزءا منها أو تجاوز الدخول المصرح به إليها أو استمر فيها بعد علمه بذلك. ورتبت تلك المادة عقوبة اشد في حالة ما إذا ترتب على هذا الدخول إلغاء أو تغيير أو تعديل أو تشويه أو إتلاف أو نسخ أو تدمير أو نشر أو إعادة نشر بيانات أو معلومات إلكترونية مخزنة في النظام المعلوماتى أو وسائل تقنية المعلومات أو تدمير ذلك النظام أو وسائل تقنية المعلومات. وبغية منح المعلومات والبيانات الشخصية حماية أكبر فقد شددت العقوبة إذا كانت البيانات أو المعلومات هي من أصابها التشويه أو التلف أو النسخ أو النشر أو إعادة نشر.وتناولت المادة (6) حالة الدخول العمدي دون وجه حق للحصول على بيانات أو معلومات حكومية سرية بطبيعتها أو بموجب تعليمات صادرة بذلك، ويعتبر في حكم البيانات والمعلومات الإلكترونية الحكومية السرية، المعلومات والبيانات السرية الخاصة بالمصارف والمؤسسات المالية. أما المادة (8) من ذات القانون فقد جرمت الاعتراض العمدي غير القانوني للمعلومات والبيانات المرسلة عبر الشبكات أو التنصت عليها. وتماشيا مع الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، والاتجاه العام فقد قرر هذا القانون في المادة (29) منه

---

(1) نص هذا القانون منشور على موقع هيئة تقنية المعلومات العمانية http://www.ita.gov.om

المسئولية الجنائية للأشخاص الاعتبارية إذا ارتكبت الجريمة باسمه أو لحسابه من قبل رئيس أو أحد أعضاء مجلس إدارته أو مديره أو أي مسئول آخر يتصرف بتلك الصفة أو بموافقته أو بتستر أو بإهمال جسيم منه.

- المرسوم السلطاني رقم 2008/69 بإصدار قانون المعاملات الإلكترونية[1]، يتضمن هذا القانون مجموعة الضمانات للبيانات الشخصية الخاصة بموجب الفصل السابع المعنون بـ(حماية البيانات الخاصة بالمواد (43 – 49) ومن أبرز تلك الضمانات:

- عدم جواز جمع بيانات شخصية مباشرة من الشخص الذي تجمع عنه البيانات أو من غيره دون موافقة صريحة من الشخص صاحب البيانات،إلا في الأحوال المبينة قانوناً، وسواء كانت الجهة التي تقوم بجمع تلك البيانات جهة حكومية أو مقدم خدمات تصديق وهو وفقا للتعريف الوارد بهذا القانون (أي شخص أو جهة معتمدة أو مرخص له / لها بالقيام بإصدار شهادات تصديق إلكترونية أو أية خدمات آخرى متعلقة بها وبالتوقيعات الإلكترونية)

- إلزام مقدموا خدمات التصديق باتباع الإجراءات المناسبة لضمان سرية البيانات الشخصية التي في عهدتهم ،وعدم إفشاء أو تحويل أو إعلان أو نشر تلك البيانات لأي غرض مهما كان إلا بموافقة مسبقة من الشخص الذي جمعت عنه البيانات.

- عدم جواز معالجة البيانات الشخصية إذا كانت تلك المعالجة تسبب ضرراً لهم أو تنال من حقوقهم أو حرياتهم،

- ضمان مستوى كافي من الحماية البيانات الشخصية عند تحويلها إلى الخارج.

وقد تضمن الفصل التاسع من هذا القانون (المواد 52 – 54) نصوص

---

(1) نص هذا القانون منشور على موقع هيئة تقنية المعلومات العمانية http://www.ita.gov.om

عقابية والتي تناولت أفعال إتلاف النظم المعلوماتية واختراقها،والعبث بالتوقيعات الإلكترونية والاستخدام غير المشروع لها والتزوير المعلوماتي وفك التشفير وغيرها من الجرائم .

2- دولة الأمارات العربية المتحدة: اتخذت عدة تدابير تشريعية في مجال حماية المعلومات وسريتها، ومكافحة الجريمة المعلوماتية بشكل عام. ومن أبرزها :

- القانون الاتحادي مكافحة جرائم تقنية المعلومات رقم 2 لسنة 2006، ويتألف هذا القانون من (29) مادة، وتناولت المادة (2) منه الدخول أو البقاء غير القانوني داخل النظام المعلوماتي وشددت العقوبة إذا ما ترتب على هذه الدخول إتلاف أو نشر أو إعادة نشر لبيانات أو معلومات شخصية، في حين تناولت المادة (22) حالة الدخول غير القانوني إلى موقع أو نظام الكتروني مباشرة أو عن طريق الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات بقصد الحصول على بيانات أو معلومات حكومية سرية إما بطبيعتها أو بمقتضى تعليمات صادرة بذلك. أما المادة(8) فقد تناولت أفعال التنصت أو التقط أو الاعتراض العمدي دون وجه حق لما هو مرسل عن طريق الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات.وأضفى هذا القانون حماية للحياة الخاصة حيث جرمت المادة (16) الاعتداء على أي من المبادئ أو القيم الأسرية أو نشر أخباراً أو صورا تتصل بحرمة الحياة الخاصة أو العائلية للأفراد، ولو كانت صحيحة، عن طريق الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات.

- قانون حماية البيانات الشخصية 2007: يطبق هذا القانون في نطاق مركز دبي المالي العالمي، ويوفر من خلال المواد (8) و (10) الحماية للبيانات والمعلومات الشخصية المعالجة آليا على غرار التشريعات الأوروبية الخاصة بحماية البيانات الشخصية قرار الأمم المتحد لسنة 1990 والاتفاقية الأوروبية 1981 بشأن حماية معلومات الأفراد المعالجة آليا.

3- جمهورية السودان: شهدت السودان في عام 2007 حركة تطوير للبنية التشريعية للتصدي للجرائم المتولدة عن إساءة استعمال تقنية المعلومات وقد تضمنت تلك التشريعات نصوصاً عقابية تكفل حماية سرية المعلومات، وأبرز تلك التشريعات:

- قانون جرائم المعلوماتية لعام 2007 [1]، في سبيل مكافحة الجرائم المعلوماتية قامت السودان في 20 يونيو 2007 بإصدار هذا القانون والذي يتألف من (30) مادة موزعة على تسع فصول تضم. وقد تضمن الفصل الثاني مجموعة جرائم نظم ووسائط وشبكات المعلومات وهي (دخول المواقع وأنظمة المعلومات المملوكة للغير، دخول المواقع وأنظمة المعلومات من موظف عام، التنصت أو التقاط أو اعتراض الرسائل، جريمة دخول المواقع عمداً بقصد الحصول على بيانات أو معلومات أمنية، إيقاف أو تعطيل أو إتلاف البرامج أو البيانات أو المعلومات، إعاقة أو تشويش أو تعطيل الوصول للخدمة.) [2] بالإضافة إلى تلك الجرائم فقد جرم بالمادة (12) الحصول على أرقام أو بيانات بطاقات الائتمان بقصد استخدامها في الحصول على بيانات الغير أو أمواله أو ما تتيحه تلك البيانات أو الأرقام من خدمات.

- قانون المعاملات الإلكترونية لسنة 2007[3] : صدر هذا القانون في 14 يونيو 2007 يضفي هذا القانون هو الآخر نوعا من الحماية للمعلومات السرية، حيث تنص المادة (28) منه على معاقبة كل من يقوم بـ (

---

(1) نص القانون منشور على موقع الإلكتروني للبنك المركزي السوداني http://www.cbos.gov.sd

(2) تنص المادة (4) من قانون الجرائم المعلوماتية السوداني لسنة 2007 على أنه (كل من يدخل موقعاً أو نظام معلومات دون أن يكون مصرحاً له ويقوم :

(أ) بالإطلاع عليه أو نسخه يعاقب بالسجن مدة لا تجاوز سنتين أو بالغرامة أو بالعقوبتين معاً ،

(ب) بإلغاء بيانات أو معلومات ملكاً للغير أو حذفها أو تدميرها أو إفشائها أو إتلافها أو تغييرها أو إعادة نشرها أو تغيير تصاميم الموقع أو إلغائه أو شغل عنوانه ، يعاقب بالسحن مدة لا تجاوز أربع سنوات أو بالغرامة أو بالعقوبتين معاً.)

- وتنص المادة (6) من ذات القانون على أنه (كل من يتنصت لأي رسائل عن طريق شبكة المعلومات أو أجهزة الحاسوب وما في حكمها أو يلتقطها أو يعترضها ، دون تصريح بذلك من النيابة العامة أو الجهة المختصة أو الجهة المالكة للمعلومة يعاقب بالسجن مدة لا تتجاوز ثلاث سنوات أو بالغرامة أو بالعقوبتين معاً .)

(3) نص القانون منشور على موقع الإلكتروني للبنك المركزي السوداني http://www.cbos.gov.sd

كشف مفاتيح التشفير المودعة بمكتب التشفير ، كشف معلومات مشفرة مخزنة لديه في الأحوال في غير الأحوال المصرح ، إساءة استخدام المعلومات المخزنة لديه، الاطلاع على المعلومات السرية دون ترخيص أو إفشائها.

4-المملكة المغربية: بغية سد الفراغ التشريعي في مجال مكافحة الجرائم المعلوماتية وحماية المعلومات اتخذ المشرع المغربي التدابير التشريعية الآتية:

- القانون رقم 03-07 المتعلق بالإخلال بسير نظم المعالجة الآلية للمعطيات[1]: صدر هذا القانون بتاريخ 11 نوفمبر 2003 وبمقتضى هذا القانون أضيف إلى القانون الجنائي المغربي باب عاشر بعنوان المس بنظم المعالجة الآلية للمعطيات (المواد-607 إلى 11-607)، وأهم الأفعال المجرمة في تلك المواد هي (الدخول الاحتيالي إلى مجموع أو بعض نظام للمعالجة الآلية للمعطيات، البقاء في نظام للمعالجة الآلية للمعطيات بعد الدخول خطأ فيه، حذف أو تغيير المعطيات المدرجة في نظام المعالجة الآلية للمعطيات أو التسبب في اضطراب في سيره، العرقلة العمدية لسير نظام المعالجة الآلية للمعطيات أو إحداث خلل فيه، إدخال معطيات في نظام للمعالجة الآلية للمعطيات أو إتلافها أو حذفها منه أو تغيير المعطيات المدرجة فيه، أو تغيير طريقة معالجتها أو طريقة إرسالها بشكل احتيالي.)

- القانون رقم 08- 09 المتعلق بحماية الأشخاص الذاتيين تجاه معالجة المعطيات ذات الطابع الشخصي[2]: أدراك المشرع المغربي حجم المخاطر التي تتعرض لها البيانات الاسمية أو الشخصية التي يتم التعامل بشأنها إلكترونياً، لذا فإنه وعلى غرار العديد من دول المجموعتين اللاتينية والأنجلوامريكية التي سبق الإشارة إليها، أصدر هذا القانون بتاريخ 18 فبراير 2009، ويهدف وفقا للمادة الأولى منه إلى تحقيق حماية فعالة للبيانات

(1) نص القانون الجنائي المغربي منشور على الموقع الإلكتروني لوزارة العدل المغربية

http://www.justice.gov.ma/

(2) نص هذا القانون منشور على الموقع الإلكتروني لوزارة العدل المغربية http://www.justice.gov.ma/

الشخصية وسـريتها، ويتألف هذا القـانون مـن (67) مـادة موزعـة عـلى ثمانيـة أبـواب. وبنظـرة عامـة فقـد تضـمن هـذا القـانون عـدة ضـمانات ومبـادئ الأساسـية لحمايـة المعلومات والبيانات الشخصية المعالجة آليا مثـل؛ مبـدأ المشـروعية والنزاهـة في جمـع المعلومـات ، مبـدأ الصـحة، مبـدأ تحديـد الغايـة، مبـدأ وصـول الأشـخاص المعنيـين إلي الملفات،مبدأ الأمن والتي سبق وأن بيناها عند تناولنا لقرار الأمم المتحـدة لسـنة 1990، والاتفاقيـة الأوروبيـة لسـنة 1981 بخصـوص حمايـة معلومـات الأشـخاص مـن مخـاطر المعالجة الآلية وإليها نحيـل. وقـد ألزمـت المـواد مـن (23 إلى 26) المسـئول عـن جمـع البيانات والمعلومات الشخصية بضمان سلامتها وسـريتها خلال معالجاته إلكترونياً،حيـث تنص المادة 23 على أنه (يجب على المسـئول عـن المعالجـة القيـام بـالإجراءات التقنيـة والتنظيمية الملائمة لحماية المعطيات ذات الطابع الشخصي من الإتـلاف العـرضي أو غـير المشـروع أو الضياع العرضي أو التلف أو الإذاعة أو الولوج غير المرخص، خصوصاً عنـدما تستوجب المعالجة إرسال معطيات عبر شبكة معينة.....)

المطلب الثالث

جهود مملكة البحرين التشريعية لحماية المعلومات الإلكترونية ومواجهة الجرائم الماسة بسريتها

يسلط هذا المطلب الضوء على الوضع الحالي لحماية البيانات والمعلومات في التشريع البحريني والتدابير التشريعية التي اتخذها المشرع في سبيل ضمان الحماية اللازمة للمعلومات في البيئة الإلكترونية.

الفرع الأول

الوضع الحالي لحماية المعلومات الإلكترونية ومواجهة الجرائم الماسة بسريتها

كفل المشرع البحريني نوعا من الحماية الجنائية لسرية المعلومات إما بمقتضى نصوص قانون العقوبات، مثال أسرار الدفاع، أو بموجب قانون خاص مثل قانون حماية الأسرار التجارية، أو بنصوص عقابية تضمنتها بعض التشريعات بمناسبة تنظم موضوع معين مثل القانون الخاص بالإحصاء والتعداد ، ولكن هل تلك القوانين أو النصوص بحالتها القائمة كفيلة بالتصدي لصور الجرائم الحديثة التي تمس بسرية المعلومات المعالجة إلكترونياً؟ هذا ما سنبينه من خلال هذا الجزء من البحث.

أولا : القواعد القانونية الخاصة بحماية أسرار الدفاع:

عرفت المادة (145) من قانون العقوبات البحريني لسنة 1976 أسرار الدفاع بأنها (1 – المعلومات الحربية والسياسية والاقتصادية والصناعية التي لا يعلمها بحكم طبيعتها إلا الأشخاص الذين لهم صفة في ذلك والتي تقضي مصلحة الدفاع عن الدولة أن تبقى سرا على من عداهم .

2 – المكاتبات والمحررات والوثائق والرسوم والخرائط والتصميمات وغيرها من الأشياء التي قد يؤدي كشفها إلى إفشاء معلومات مما أشير إليه في الفقرة السابقة والتي تقضي مصلحة الدفاع عن الدولة أن تبقى سرا على غير من يناط بهم حفظها أو استعمالها .

3 – الأخبار والمعلومات المتعلقة بالقوات المسلحة وتشكيلاتها وتحركاتها وعتادها وتموينها وأفرادها وغير ذلك مما له مساس بالشئون العسكرية والخطط الحربية ما لم يكن قد صدر إذن كتابي من القائد العام لقوة دفاع الدولة أو ممن ينيبه بنشره أو إذاعته.

4 – الأخبار والمعلومات المتعلقة بالتدابير والإجراءات التي تتخذ لكشف الجنايات المنصوص عليها في هذا الفصل وضبط الجناة ، وكذلك الأخبار والمعلومات الخاصة بسير التحقيق والمحاكمة إذا حظرت سلطة التحقيق أو المحكمة المختصة إذاعتها .)

وبموجب المادة (126) من ذات القانون فأنه (يعاقب بالإعدام من سلم أو أفشى على أي وجه وبأية وسيلة إلى دولة أجنبية أو إلى أحد ممن يعملون لمصلحتها سرا من أسرار الدفاع أو توصل بأية طريقة إلى الحصول على سر من هذه الأسرار بقصد تسليمه أو إفشائه لدولة أجنبية أو لأحد ممن يعملون لمصلحتها.

فيما نصت المادة (127) من ذات القانون على أنه (يعاقب بالسجن مدة لا تزيد على عشر سنوات كل موظف عام أو مكلف بخدمة عامة أفشى سرا من أسرار الدفاع أئتمن عليه.وتكون العقوبة السجن إذا وقعت الجريمة في زمن الحرب.)

وتنص المادة (128) من ذات القانون على أنه (يعاقب بالحبس مدة لا تقل عن ستة أشهر ولا تزيد على خمس سنين :1 – من حصل بأية وسيلة غير مشروعة على سر من أسرار الدفاع عن البلاد ولم يقصد تسليمه أو إفشاءه لدولة أجنبية أو لأحد ممن يعملون لمصلحتها .

2 – من أذاع عمدا بأية طريقة سرا من أسرار الدفاع .

3 – من نظم أو استعمل أية وسيلة من وسائل الاتصال بقصد الحصول على سر من أسرار الدفاع عن البلاد أو تسليمه أو إذاعته.)

يلاحظ أن النصوص المتقدمة اتسمت بنوع من المرونة بحيث تشمل كل أفعال إفشاء أسرار الدفاع أو الحصول عليها وأياً كانت الوسيلة المستخدمة في ارتكاب الجريمة، مما يجعلها صالحة للتطبيق على جرائم الحصول على سر من أسرار الدفاع عن طريق اختراق الأنظمة المعلوماتية المخزن بها تلك الأسرار، أو من خلال الاعتراض غير القانوني أو التقاط تلك الأسرار خلال انتقالها بواسطة الشبكات لالكترونية. وعلى الرغم من تلك الحماية التي توفرها النصوص المتقدمة للأسرار الدفاع، إلا أنها لم تتضمن حالات الدخول غير القانوني أو تجاوز التصريح في البقاء داخل النظام المعلوماتي، أو حتى محاولات الدخول أو الاختراق لتلك النظم رغم ما يشكله ذلك من تهديد خطير لأسرار الدفاع المخزنة داخل النظام المعلوماتي، فكما سبق الإشارة إليه في مواضع سابقة من هذا البحث، من أن محاولات الدخول غير المشروع وإن لم تتم، إلا أنها قد تؤدي إلى إحداث ثغرات في النظم المعلوماتية يمكن ان يتسلل من خلالها أي مخترق آخر.

ثانياً: القواعد القانونية الخاصة بحماية أسرار الحياة الخاصة:

الحق في الحياة الخاصة هو أحد الحقوق الأساسية للإنسان التي تتكفل الدساتير والقوانين برعايتها وحمايتها، وذلك بهدف صون كرامة الإنسان واحترام خصوصيته، والحيلولة دون التطفل عليه وانتهاك أسراره ومختلف جوانب حياته الخاصة.

ويعرف البعض الحق في الحياة الخاصة أو الحرمة الشخصية بأنه (حق الأفراد أو الجماعات أو المؤسسات في أن يقرروا بأنفسهم زمن وكيفية ومدى نقل المعلومات عن أنفسهم إلى الآخرين، والخصوصية، منظورا إليها من علاقة الفرد بالمشاركة الاجتماعية، هي انسحاب الفرد الطوعي والمؤقت من المجتمع العام عبر وسائل مادية أو نفسية) [1]

---

(1) د. صالح جواد الكاظم، مباحث في القانون الدولي- الطبعة الأولى- دار الشؤون الثقافية العامة - بغداد 1991 - ص 136

بينما يعرفه البعض الآخر بأنه (حق الفرد في أن يحدد بنفسه ما يتقاسمه مع الآخرين في أفكاره وعواطفه والحقائق المتعلقة بحياته الشخصية)[1]

وفي محاولة لتحديد الأمور التي تدخل في نطاق الحياة الخاصة، قرر القضاء الفرنسي أنه يعد من الأمور التي تدخل في نطاق الحق في الحياة الخاصة للفرد، حالة الشخص العائلية والعاطفية والجسمانية والنفسية والعقلية والدينية والفلسفية والروحية. كما قرر بأن (الحياة العائلية كالزواج والطلاق والبنوة ، والحياة العاطفية ، والصور الشخصية، والذمة المالية ، وما يدفعه من ضرائب ، وكيفية قضائه لأوقات فراغه ، تعد من الحياة الخاصة ، وكذلك ، حق الشخص في الاسم والصوت وفي الشرف والاعتبار وفي سيرة حياته الداخلية والروحية)[2]

وبدوره فقد أولى المشرع البحريني الحياة الخاصة اهتماما خاصاً وكفل لها الحماية بموجب الدستور والقانون، حيث تنص المادة (25) الدستور البحريني المعدل عام 2002 على أن (للمساكن حرمة، فلا يجوز دخولها أو تفتيشها بغير إذن أهلها إلا استثناء في حالات الضرورة القصوى التي يعينها القانون، وبالكيفية المنصوص عليها فيه .)

وتنص المادة 26 منه على أن (حرية المراسلة البريدية والبرقية والهاتفية والإلكترونية مصونة، وسريتها مكفولة، فلا يجوز مراقبة المراسلات أو إفشاء سريتها إلا في الضرورات التي يبينها القانون، ووفقا للإجراءات والضمانات المنصوص عليها فيه.)

وقد ورد بالمذكرة التفسيرية لهذا الدستور في معرض تبرير التعديلات التي أجريت على المادة (26) ما نصه (أمام التقدم العلمي الذي سيطرت فيه

---

(1) د. محمد سامي الشوا، الغش المعلوماتي كظاهرة اجرامية مستحدثة، ورقة عمل مقدمة للمؤتمر السادس للجمعية المصرية للقانون الجنائي، القاهرة، 25-28 تشرين أول / أكتوبر 1993. صـ 170

(2) د.يونس عرب - بحث بعنوان الخصوصية وحماية البيانات - مرجع سابق منشور على الموقع الإلكتروني doc.abhatoo.net.ma/IMG/doc/dro3.doc صـ 49

الثورة المعلوماتية والأجهزة الإلكترونية الحديثة على المجتمعات المعاصرة، ونظرا إلى ما يمثله ذلك من خطورة على حرمة الحياة الخاصة للمواطنين، عدلت هذه المادة لتضيف إلى وسائل حماية الحياة الخاصة عدم جواز مراقبة المراسلات الإلكترونية إلا بضوابط معينة، شأنها في ذلك شأن المراسلات البريدية والبرقية والهاتفية)[1]

ويتضح مما سبق حرص المشرع الدستوري على ضمان أكبر قدر من الحماية للحياة الخاصة ضد ما يهددها من أخطار تقليدية أو حديثة كأثر للتقدم العلمي وتكنولوجيا المعلومات.ومن صور الحماية الجنائية للحياة الخاصة ما يأتي:

فقد نصت المادة (370) من قانون العقوبات على أنه (يعاقب بالحبس مدة لا تزيد على ستة أشهر وبالغرامة التي لا تجاوز خمسين دينارا أو بإحدى هاتين العقوبتين من نشر بإحدى طرق العلانية أخبارا أو صورا أو تعليقات تتصل بأسرار الحياة الخاصة أو العائلية للأفراد ولو كانت صحيحة إذا كان من شأن نشرها الإساءة إليهم).

وتنص المادة (371) على أنه (يعاقب بالحبس مدة لا تزيد على سنة أو بالغرامة التي لا تجاوز مائة دينار من كان بحكم مهنته أو حرفته أو وضعه أو فنه مستودع سر فأفشاه في غير الأحوال المصرح بها قانونا أو استعمله لمنفعته الخاصة أو لمنفعة شخص آخر ، وذلك ما لم يأذن صاحب الشأن في السر بإفشائه أو استعماله،وتكون العقوبة السجن مدة لا تزيد على خمس سنين إذا كان الجاني موظفا عاما أو مكلفا بخدمة عامة واستودع السر أثناء أو بسبب أو بمناسبة تأديته وظيفته أو خدمته).

---

(1) نص المادة (26) من دستور مملكة البحرين لعام 1973 قبل التعديل (حرية المراسلة البريدية والبرقية والهاتفية مصونة، وسريتها مكفولة، فلا يجوز مراقبة المراسلات أو إفشاء سريتها إلا في الضرورات التي يبينها القانون، ووفقا للإجراءات والضمانات المنصوص عليها فيه.)،

وتنص المادة (372) على أنه (يعاقب بالغرامة التي لا تجاوز عشرين دينارا من فض رسالة أو برقية بغير رضا من أرسلت إليه أو استرق السمع في مكالمة تليفونية .ويعاقب الجاني بالحبس مدة لا تزيد على ستة أشهر أو بالغرامة التي لا تجاوز خمسين دينارا إذا أفشى الرسالة أو البرقية أو المكالمة لغير من وجهت إليه ودون إذنه متى كان من شأن ذلك إلحاق ضرر بالغير .)

وتنص المادة (213) من ذات القانون على أنه (يعاقب بالحبس أو بالغرامة كل موظف عام أخفى رسالة سلمت للبريد أو أتلفها أو فتحها أو سهل ذلك لغيره. ويسري هذا الحكم على الرسائل السلكية واللاسلكية .)

وتعليقا على النصوص السابقة نلاحظ أن :

أ- أن المادة 370 اقتصرت على تجريم صورة واحدة من صور الاعتداء على الحياة الخاصة للأفراد وهي النشر أو الإذاعة بإحدى الطرق العلنية لأخبارا أو صور أو تعليقات تتصل بأسرار الحياة الخاصة أو العائلية للأفراد، ويعد ذلك أهم مثالب تلك المادة، حيث أنها على هذا النحو تكون قاصرة وعاجزة عن توفير الحماية المنشودة للحياة الخاصة للأفراد في وقت ازداد فيه الاعتماد على الحاسبات الآلية وشبكات الاتصال في جمع وتخزين ومعالجة ونقل المعلومات والبيانات الخاصة بالأشخاص، وما رافق ذلك من ازدياد احتمالات تعرض تلك المعلومات والبيانات لصور مختلفة من الاعتداء لا تشملها المادة السابقة مثل إساءة الاستخدام، والوصول إليها بطريق غير المشروع والاطلاع عليها والعبث بها من قبل المتطفلين، ولصوص المعلومات.

ومثال للتوضيح: إذا قام أحد المتطفلين باختراق جهاز الحاسب الآلي الخاص بأحد الأشخاص والذي يمثل وعاءً أو مستودعاً لأسراره الشخصية أو العائلية من صور ومعلومات عن وضعه المادي أو الصحي أو انتمائه السياسي، واقتصر فعل المتطفل على الاطلاع على ما يحتويه الجهاز المخترق من معلومات وبيانات والعبث به ولم يقم بنشر تلك المعلومات أو الصور.

فإنه في هذه الحالة لا يمكن تطبيق أحكام المادة (370) من قانون العقوبات لأن الشخص المتطفل لم يأتِ الفعل المجرم في تلك المادة وهو النشر بإحدى طرق العلانية للأخبار أو الصور المتعلقة بأسرار الحياة الخاصة أو العائلية للأفراد التي توصل إليها، مع أن ما قام به يشكل انتهاكاً بحق الفرد في أن يحدد بنفسه ما يتقاسمه مع الآخرين في أفكاره وعواطفه والحقائق المتعلقة بحياته الشخصية. الأمر الذي يؤكد على ضرورة تدخل تشريعي لإجراء تعديلات تشريعية أو استحداث نصوص جديدة تتوائم مع ما يشهده المجتمع من تطور وتقدم تقني، وعلى نحو يكفل قدر اكبر من الحماية للحياة الخاصة من هذه الحالة ومن غيرها من حالات الاعتداء التي قد تطرأ مستقبلا.

ب- يتعلق حكم المادة (371) بجريمة إفشاء أو استعمال الأسرار التي توصل إليه شخص ما بحكم مهنته أو حرفته أو وضعه أو فنه، ولم يحدد صور محددة لفعل الإفشاء أو طريق الاستعمال وعليه يشمل كل صور الإفشاء أو الاستعمال سواء التقليدي منها أو الإلكتروني، وهو ما لا يثير إشكالية بشأن تطبيق هذا النص على أي فعل من شأنه تحقيق النتيجة الإجرامية.

ج- فيما يتعلق بتطبيق حكم المادة 372 من قانون العقوبات على المراسلات الإلكترونية التي تتم بواسطة شبكة الانترنت مثل البريد الإلكتروني[1]،يرى البعض أن المراسلات الإلكترونية ذات طبيعة تختلف عن المراسلات العادية ويتمثل هذا الاختلاف في صعوبة تحديد المسئولية بالنسبة لمرسل الرسالة، وبالنسبة لمزود الخدمة فإنه يصعب توجيه المسئولية إليه لأنه يتعذر عليه التحكم أو مراقبة المستخدمين حيث تقتصر مسئوليته على ما يقوم هو بإنتاجه أو نشره، وعلى هذا الأساس فإن القوانين التي تعاقب على

---

(1) البريد الإلكتروني هو عبارة عن نظام لتبادل المعلومات سواء كانت نصيه أو صوتية أو أفلام وصور أو برامج وتطبيقات كمبيوتر ويشترط لاستخدام البريد الإلكتروني أن يكون من المرسل والمستقبل عنوان بريد إلكتروني وكمبيوتر واشتراك في شبكة الانترنت- موقع الإلكتروني http://www.tcl jeeran com/mail.htm

الاعتداءات التي تقع على المراسلات البريدية العادية لا يمكن تطبيقها على المراسلات الإلكترونية التي تتم بواسطة الانترنت، وبالتالي تظهر الحاجة إلى وجود قوانين توفر الحماية اللازمة لمستخدمي الشبكات الإلكترونية وحماية مراسلاتهم الإلكترونية التي قد تحمل أسرار أو معلومات تهدد حياتهم الخاصة [1].

وفي تقديري فإن المادة (75) من المرسوم بقانون رقم (48) لسنة 2002 بإصدار قانون الإتصالات البحريني أدركت هذا النقص بنصها على أنه (مع عدم الإخلال بأية عقوبة أشد ينص عليها قانون العقوبات أو أي قانون آخر, يعاقب بالغرامة التي لا تجاوز عشرة آلاف دينار كل من استخدم أجهزة أو شبكة الإتصالات بقصد :..2- التصنت على أو إفشاء سرية أية مكالمات أو بيانات تتعلق بمضمون أية رسالة أو بمرسلها أو بالمرسل إليه, ما لم يكن التصنت أو الإفشاء بموجب إذن من النيابة العامة أو أمر صادر من المحكمة المختصة.) وبموجب هذا النص فإن الحماية من التصنت أو إفشاء السرية تشمل أية مكالمات ومضمون أية رسالة بما فيها الرسائل الإلكترونية أو بمرسلها أو بالمرسل إليه، فالعام يطلق على عمومه ما لم يرد ما يخصصه.

ثالثا: القواعد القانونية الخاصة بحماية المعلومات والبيانات المتعلقة بالإحصاء والتعداد:

تنص المادة (6) من المرسوم بقانون رقم (7) لسنة 1977 في شأن الإحصاء والتعداد من أنه (يعاقب بالحبس مدة لا تزيد على سنة أو بغرامة لا تتجاوز ستمائة دينار أو بالعقوبتين معا كل من أخل بسرية الإحصائيات أو أفشى بيانا من البيانات أو سرا من أسرار الصناعة أو التجارة أو غير ذلك من أساليب العمل التي يكون قد اطلع عليها بمناسبة عمله في الإحصاء. كما يعاقب بالحبس مدة لا تزيد على ستة أشهر أو بغرامة لا تتجاوز ثلاثمائة دينار:-

---

(1) د. احمد حسام طه تمام - الحماية الجنائية لتكنولوجيا الاتصالات (دراسة مقارنة) - دار النهضة العربية 2002م - صـ 32.

أ- كل من حصل بطريق الغش أو التهديد أو الإيهام بأية وسيلة آخرى على بيانات أو معلومات سرية بشأن الإحصاءات والتعدادات أو شرع في ذلك.

ب- كل من أجرى إحصاء أو تعدادا أو استفتاء على خلاف أحكام هذا القانون والقرارات الصادرة تنفيذا له.

ج- كل من نشر أو تسبب في نشر إحصاءات أو تعدادات غير صحيحة مع علمه بذلك...)

نلاحظ أن المادة السابقة بصيغتها تلك، تكون قد شملت كافة صور الأفعال التي تخل بسرية المعلومات المشار إليها في المادة السابقة والتي قد تقع في مجال تكنولوجيا المعلومات من خلال الدخول غير القانون للنظام المعلوماتي، أو الاعتراض القانوني أو التقاط تلك البيانات خلال عملية نقلها.

رابعاً: القواعد القانونية الخاصة بحماية الأسرار التجارية:

تماشياً مع أحكام الاتفاقيات الدولية في مجال التجارة مثل اتفاقية تأسيس منظمة التجارة، اتفاقية باريس لحماية الملكية الصناعية، اتفاقية إنشاء المنظمة العالمية للملكية الفكرية (الويبو)[1]، والتي تتضمن إلزام للدول الموقعة عليها بضمان الحماية الأزمة للأسرار التجارية، ونظراً لأهمية السرية في مجال الأعمال التجارية، والتي قد تمنح صاحب المصلحة في المعلومة السرية ميزة تنافسية في الأسواق، وما يترتب على انتهاك سرية تلك المعلومة من فوات تلك الميزة عليه، فصلا عما يتبع ذلك من خسائر مادية ، قد توصف في بعض الأحيان بالفادحة، فقد أصدر المشرع البحريني القانون رقم (7)

---

(1) صادقت مملكة البحرين على وثيقة تأسيس منظمة التجارة الدولية بموجب المرسوم بقانون رقم (7) لسنة 1994، وانضمت إلى اتفاقية باريس لحماية الملكية الصناعية بموجب المرسوم بقانون رقم (31) لسنة 1996، وانضمت إلى اتفاقية إنشاء المنظمة العالمية للملكية الفكرية (الويبو) بالمرسوم رقم (1) لسنة 1995

لسنة 2003 بشأن حماية الأسـرار التجاريـة، وقـد بينـت المـادة (1) مـن هـذا القـانون المقصود بالأسـرار التجارية وعناصرها حيث تـنص عـلى أنـه : (يحظـر عـلى كـل شـخص طبيعي أو اعتباري إفشاء المعلومات التي تكون بحوزته إذا اتسمت بما يلي :-

أ- إذا كانت سـرية ، وتتحقق هذه السـرية إذا كانت المعلومات في صـورتها النهائيـة أو في مفرداتها الدقيقة غير معروفة، أو غير متداولة، وليس مـن السـهل الحصـول عليهـا لدى المشتغلين عادة بهذا النوع من المعلومات.

ب- إذا كانت ذات قيمة تجارية نظراً لكونها سـرية.

ج- إذا كانت تعتمد في سـريتها على مـا اتخـذه حائزهـا القـانوني مـن تـدابير فعالـة للحفاظ عليها.

وفي تطبيق أحكام هذا القانون تعد المعلومات التي تتوافر فيهـا السـمات المنصـوص عليها في البنود السابقة أسـراراً تجارية)

كـما مـد نطـاق حمايـة السـرية وفقـا للـمادة (2) مـن ذات القـانون إلى البيانـات والاختبارات السـرية التي كانت نتيجة جهود معتبرة ، والتي تقدم إلى الجهات المختصـة بناء على طلبها للموافقة على تسويق المنتجـات الصيدلية أو الزراعيـة الكيميائيـة التـي تستخدم فيها كيانات كيميائية جديدة.

ولقد عاقب هذا القانون على انتهاك سـرية المعلومات التجارية بنص عام يشمل أي وسيلة غير مشـروعة تقليدية كانت أم الكترونية يقوم من خلالها الجاني بالكشـف عـن الأسـرار التجارية المحمية طبقاً لأحكام القانون أو بحيازتهـا أو باسـتخدامها مـع اشـتراط علم الجاني بسـريتها أو بأنه متحصلة غير مشـروعة. حيـث تـنص المـادة (7) مـن ذات القانون على أنه (مع عدم الإخلال بأية عقوبة أشد ينص عليها أي قانون آخـر ، يعاقـب بالحبس مدة لا تقل عن ثلاثة أشهر ولا تزيد على سنة وبغرامـة لا تقـل عـن خمسـمائة دينـار ولا تجـاوز ألفـي دينـار أو بإحـدى هـاتين العقـوبتين كـل مـن قـام بوسـيلة غـير

مشروعة بالكشف عن الأسرار التجارية المحمية طبقاً لأحكام هذا القانون أو بحيازتها أو باستخدامها مع علمه بسريتها وبأنها متحصلة عن تلك الوسيلة.ويجوز للمحكمة أن تأمر بنشر الحكم في صحيفة محلية يومية مرة واحدة أو أكثر على نفقة المحكوم عليه...)

وبعد استعراض ما تقدم، نخلص إلى أن التشريع البحريني قد تضمن،بعض النصوص العقابية قد تصلح لحماية سرية المعلومات من بعض صور الأفعال الماسة بسريتها، إلا أنها لا تشملها جميعها وتحديد تلك التي تقع في مجال تكنولوجيا المعلومات.

كما نلاحظ وجود فراغ تشريعي لمكافحة الجرائم المعلوماتية في مملكة البحرين، فضلا عن الحاجة إلى تشريع خاص بحماية البيانات الشخصية المعالجة آلياً من المخاطر التي تتهددها اقتضاءً بالتوجه العام لكثير من دول العالم.

الفرع الثاني

تطوير البنية لتشريعية لحماية المعلومات الإلكترونية ومواجهة الجرائم الماسة بسريتها

قطعت مملكة البحرين أشوطاً كبيرة في مجال الاعتماد على تكنولوجيا المعلومات في مختلف المجالات مثل التعليم الإلكتروني والتعليم عن بعد، ومشروع الحكومة الإلكترونية، وفي مجال الخدمات المالية والمصرفية مثل التجارة الإلكترونية والتعاملات المالية والبنكية الإلكترونية. وحققت مراكز متقدمة على المستوى العالمي والإقليمي في هذا المجال، فكما سبق الإشارة احتلت مملكة البحرين المركز الـ13 عالمياً والأول خليجيا وعربيا في مجال الخدمات الإلكترونية وفقا لمؤشر الأمم المتحدة للحكومة الإلكترونية لسنة 2010[1]، ووفقاً لأحدث تقرير لمؤشر الأمم المتحدة للحكومة الإلكترونية الصادر عام 2012م فقد حققت المملكة تقدما في مجال الخدمات الإلكترونية حيث احتلت الترتيب السابع على مستوى دول العالم، والثالث آسيويا، والأول على مستوى دول الإقليم[2]. ويتطلب هذا التقدم والاعتماد المتنامي على تقنية المعلومات، تطوراً مماثلاً على المستوى التشريعي الذي يكفل للمعلومات المعالجة آلياً بمختلف أنواعها الحماية اللازمة ضد ما يتهددها من مخاطر أهمها أمن وسرية تلك المعلومات، وسبق وان بينا في مواقع متعددة من هذا البحث أن مملكة البحرين تعاني من فراغ وقصور تشريعي في مجال مكافحة الجرائم المعلوماتية وحماية البيانات المعالجة ألياً ، وهو ما قد يشكل عقبة في طريق تقدمها في مجال الخدمات الإلكترونية، نتيجة

---

(1) وكالة أنباء البحرين : http://www.bna.bh/portal/news/447185

(2) وتجدر الإشارة إلى أنه يتم التقييم بناءً على أربع مؤشرات رئيسية وهي المعلومات المتوفرة كالسياسات والوثائق القانونية وغيرها، والخدمات العامة، والمشاركة الإلكترونية، ومميرات تقنية من سمعية وبصرية.
المرجع:

http://www.bahrain.bh/pubportal/newsletter/03-12/html/ar/03-Ini1.html

لخشية الأفراد والمؤسسات من المساس ببياناتهم ومعلوماتهم الخاصة وبالتالي عزوفهم عن الاعتماد على تلك الخدمات. وإدراكاً من المشرع البحريني بأهمية معالجة هذا النقص التشريعي فقد أقدم على اتخاذ عدة خطوات في اتجاه استكمال البنية التشريعية الخاصة بحماية المعلومات ومكافحة الجرائم الماسة بها أبرزها ما يأتي:

1- **مشروع قانون بشأن جرائم الحاسب الآلي:**

طرح هذا المشروع بقانون على مجلس النواب البحريني في الفصل التشريعي الثاني عام 2009 بمناسبة عرض مشروعين بقانون بهذا الشأن أحدهما قدم من قبل الحكومة، والآخر قدم من بعض أعضاء مجلس النواب.[1] ويهدف هذا المشروع وفقاً لما ورد بتقرير لجنة الشئون الخارجية والدفاع والأمن الوطني بمجلس النواب إلى تطوير قوانين المملكة بما يضمن التصدي للجرائم الناتجة عن تكنولوجيا المعلومات، نظراً لعدم كفاية النصوص العقابية والإجرائية التقليدية لمواجهة تلك الجرائم،ولتفادي التوسع في تفسير أو القياس على النصوص العقابية التقليدية لتجريم صور الجرائم المعلوماتية الحديثة وما يترتب على ذلك من إخلال جسيم بمبدأ الشرعية الجنائية. ويتألف من (27) مادة موزعة على ثلاثة فصول، فخصص الفصل الأول للجانب الموضوعي والذي يتضمن صور الجرائم المعلوماتية المختلفة مثل (الدخول غير المشروع، إتلاف بيانات الحاسب الآلي أو نظام الحاسب الآلي،الالتقاط غير المشروع، التهديد بقصد الابتزاز، إساءة استخدام الأدوات، التزوير باستخدام الحاسب الآلي، الاحتيال باستخدام الحاسب الآلي، الجرائم ذات الصلة بالمحتوى مثل المواد الإباحية من الأطفال). أما الفصل الثاني فقد خصص للجوانب الإجرائية الخاصة بالجرائم المعلوماتية مثل (الحفاظ على بيانات الحاسب الآلي والإبقاء على

(1) نص المشروعين بقانون بالإضافة إلى تقرير اللجنة المختصة ومضابط الجلسات منشورة على الموقع الإلكتروني لمجلس النواب البحريني www.nuwab.gov.bh

سلامتها، تقديم بيانات حاسب آلي ومعلومات عن المشترك، الحفاظ على بيانات خط السير والكشف الجزئي عنها، الدخول والتفتيش، الضبط والتحفظ، الأمر بتوفير معلومات، اعتراض بيانات خط السير وبيانات المحتوى، مخالفة الأمر أو التكليف.) ويشمل الفصل الثالث أحكاماً متفرقة مثل (الشروع والمساهمة، مسئولية الشخص الاعتباري..).ونبين فيما يلي أهم ما نراه من ملاحظات بشأن هذا المشروع بقانون:

أولا: الملاحظات العامة على المشروع بقانون:

أ- يعد هذا المشروع خطوة إيجابية في سبيل سد الفراغ التشريعي في مجال مكافحة الجرائم المعلوماتية ، ومن جانبي أرى أن أهم ما يميزه أنه تضمن قواعد إجرائية خاصة تتناسب مع طبيعة الجرائم المعلوماتية وطبيعة الأدلة المتحصلة عنها مثل جمع الأدلة وحفظها وتتبع خط سير البيانات.

ب- فيما يتعلق بالجانب الموضوعي الخاص بصور الجرائم المعلوماتية والتي تضمنها الفصل الأول؛ فإنه بمقارنة هذا المشروع بقانون بكل من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010 الموقعة عليها مملكة البحرين والتي سبق وأن استعرضناها وإليها نحيل، والإرشاد الخامس الصادر عن اللجنة الاقتصادية والاجتماعية لغربي أسيا (الإسكوا)[1] بخصوص للتشريعات السيبرانية، والذي اشتمل على القانون الاسترشادي المقترح من جانبها والذي تضمن الإشارة إلى الجرائم التي ينبغي أن تتضمنها التشريعات الخاصة بمكافحة الجرائم المعلوماتية وهي (التعدي على البيانات المعلوماتية،التعدي على الأنظمة المعلوماتية، إساءة استعمال الأجهزة أو البرامج المعلوماتية، جرائم الأموال، الاستغلال الجنسي للقاصرين،

---

(1) اللجنة الاقتصادية والاجتماعية لغربي أسيا (الإسكوا) هي إحدى اللجان الإقليمية الخمس في الأمم المتحدة. التي أنشئت بهدف تحقيق الأهداف الاقتصادية والاجتماعية الواردة في ميثاق الأمم المتحدة ، وقد تأسست بتاريخ 9 أغسطس 1973وتضم في عضويتها (14) بدءاً عربياً في منطقة غربي آسيا هي: البحرين (انضمت إليها بتاريخ 9/8/ 1973). الأردن والإمارات العربية المتحدة والجمهورية العربية السورية والعراق وعمان وفلسطين وقطر والكويت ولبنان ومصر والمملكة العربية السعودية واليمن والسودان. المرجع:
http //www.escwa.un org/arabic/about/main.asp

جرائم التعدي على الملكية الفكرية للأعمال الرقمية،جرائم البطاقات المصرفية والنقود الإلكترونية، الجرائم التي تمس المعلومات الشخصية، جرائم العنصرية والجرائم ضد الإنسانية بوسائل معلوماتية، جرائم المقامرة وترويج المواد المخدرة بوسائل معلوماتية، والجرائم ضد الدولة والسلامة العامة وجرائم تشفير المعلومات.)[1]، فإننا نلاحظ عدم اشتمال المشروع بقانون البحريني على بعض الجرائم التي وردت بالاتفاقية العربية أو الإرشاد الخامس للإسكوا سالف البيان، مثل (الجرائم المتعلقة بالإرهاب والمرتكبة بواسطة تقنية المعلومات، الجرائم المتعلقة بالجرائم المنظمة والمرتكبة بواسطة تقنية المعلومات، الجرائم المتعلقة بانتهاك حق المؤلف والحقوق المجاورة، الاستخدام غير المشروع لأدوات الدفع الالكترونية، جرائم العنصرية والجرائم ضد الإنسانية بوسائل معلوماتية).

لذا فإننا نقترح على المشرع البحريني،إعادة النظر في هذا المشروع بقانون في ضوء الاتفاقية العربية لعام 2010 ، واستكمال صور الجرائم المختلفة التي وردت بالاتفاقية ولم ترد بالمشروع بقانون تنفيذاً لنص المادة الخامسة من هذه الاتفاقية والتي تلتزم كل دولة طرف بتجريم الأفعال المبينة في الفصل الثاني منها وذلك وفقاً لتشريعاتها وأنظمتها الداخلية، ولما في ذلك من تيسير التعاون الدولي في مجال مكافحة الجرائم المعلوماتية وخاصة في مجال تسليم المجرمين والذي يتطلب التجريم المزدوج للجرائم المطلوب بشأنها التسليم. وكذلك الاستفادة من القانون الإرشادي الصادر عن (الإسكوا) باعتباره نموذج للتشريعات المتقدمة في مجال مكافحة جرائم المعلوماتية، وذلك بالإضافة إلى تجارب الدول التي قطعت شوطاً كبير في هذا المجال.

ثانياً: الملاحظات الخاصة بصور الجرائم الماسة بسرية المعلومات الإلكترونية موضوع البحث:

أ جريمة الدخول غير المشروع (المادة 3) : وفقا للتقرير التكميلي

---

(1) الإرشاد الخامس - الجرائم السيبرانية – صـ13 منشور على الموقع الإلكتروني /http://isper.escwa.un org

للجنة المختصة بشأن المشروعين بقانون السابقين الصادر بتاريخ 14 ديسمبر 2011، فقد تم الاتفاق على تجريم الدخول غير المشروع بالنص الآتي (يعاقب بالحبس مدة لا تزيد على سنة وبالغرامة التي لا تجاوز ثلاثين ألف دينار أو بإحدى هاتين العقوبتين، من قام عمداً بالدخول إلى نظام الحاسب آلي أو أي جزء منه.)، وبمطالعة التقرير المشار إليه نلاحظ أنه قد تم تعديل الصياغة الأولى لهذه المادة، وتم حذف عبارة (دون وجه حق) واستبدالها بكلمة (عمداً) حيث كان المادة قبل التعديل تنص على أنه (يعاقب بالحبس مدة لا تزيد على سنتين وبالغرامة التي لا تجاوز مائة ألف دينار أو بإحدى هاتين العقوبتين، من قام دون وجه حق بالدخول إلى نظام الحاسب آلي أو أي جزء منه).

ومن جانبي أرى أنه يتعين أن يتضمن النص الخاص بهذه الجريمة العبارتين معا دون حذف إحداهما ليكتمل المعنى على الوجه الصحيح والذي يقصده المشرع، لذا نقترح أن يكون نص المادة كالأتي: (يعاقب بالحبس مدة لا تزيد على ......وبالغرامة التي لا تجاوز ..... دينار أو بإحدى هاتين العقوبتين، من قام بالدخول عمداً ودون وجه حق إلى نظام الحاسب الآلي..) وتبرير ذلك؛ أن صفة العمد لا تكفي للتجريم لأن الفعل من حيث الأصل ليس مُجرّماً، فالتقني أو المبرمج يقوم بالدخول عمداً إلى النظام المعلوماتي أو بمحاولة اختراقه ولكنه يقوم بذلك بحكم عمله وبناء على تصريح ممن له السلطة القانونية على النظام وبقصد اختبار كفاءة برامج الحماية المستخدمة في حماية النظم المعلوماتية، وكذلك الحال بالنسبة لحالات الدخول العمدي إلى النظم المعلوماتية في الحالات المبينة قانوناً كحالات التفتيش.

ومن جهة آخرى فإن الاقتصار على عبارة (دون وجه حق) فقط دون استخدام كلمة (عمداً) قد يدخل نطاق التجريم حالات قد لا يقصده المشرع، مثل حالات الدخول غير العمدي، فمن دخل إلى نظام معلوماتي بالخطأ فقد دخل إلى نظام معلوماتي لا حق له بالدخول إليه، حيث أنه من

المستقر عليه في غالبية النظم القانونية التي سنت تشريعات خاصة بجرائم المعلومات إن لم يكن جميعها، تخرج حالات الدخول غير العمدي من نطاق التجريم.

وعلى الرغم من تضمن هذا المشروع بقانون تجريم حالات الدخول العمدي بطريق غير مشروع وبأية وسيلة كانت بقصد الحصول على بيانات أو معلومات أو تعديلها، أو أخذ نسخ منها أو نقلها.وشدد العقاب على حالات الدخول غير المشروع إلى النظم المعلوماتية بقصد الحصول على بيانات أو معلومات تمس الأمن الداخلي أو الخارجي للمملكة أو الأضرار باقتصادها الوطني. إلا أنه لم يتضمن إشارة إلى الدخول إلى البيانات الشخصية أو المالية والمصرفية والبنكية أو تقرير عقوبة أشد بالنسبة للدخول إليها.

ب- جريمة تجاوز التصريح بالدخول أو البقاء غير المصرح به داخل النظام المعلوماتي: يلاحظ عدم تناول النص السابق أو غيره من نصوص المشروع بقانون هذه الجريمة وهو ما يعد نقص في التجريم، يتعين تداركه.

ج- جريمة الاعتراض غير القانوني (مادة 4): تم الاتفاق على النص الأتي (يعاقب بالحبس وبالغرامة التي تجاوز مائة ألف دينار أو بإحدى هاتين العقوبتين من ألتقط عمداً، مستخدما وسائل فنية، إرسالاً غير موجه للعموم لبيانات حاسب آلي سواء كانت البيانات مرسلة من نظام حاسب آلي أو إليه أو ضمنه، ويشمل هذا الإرسال لموجات كهرومغناطيسية من نظام حاسب آلي تحمل معها هذه البيانات)

يتناول هذا النص جريمة الاعتراض غير القانوني، ونقترح إضافة عبارة (دون وجه حق) إلى هذه المادة لذات التبريرات التي سقناها في معرض التعليق على المادة الخاصة بجريمة الدخول غير القانوني. ليكون النص المقترح كالآتي (يعاقب بالحبس وبالغرامة التي تجاوز مائة ألف دينار أو بإحدى هاتين العقوبتين من التقط عمداً ودون وجه حق، مستخدما وسائل فنية، .....)

2- مشـروع بقانون بشأن ضمان حق الحصول على المعلومات[1]:

طرح هذا القانون على مجلس النواب البحريني خلال دور الانعقاد الثالث من الفصل التشريعي الثاني في عام 2008، ويهدف هذا المشـروع بقانون وفقا لمبررات تقديمه إلى إيجاد تشـريع يضمن للمواطن الحق في الحصول على المعلومات المشـروعة، وبث روح الشفافية والإفصاح في المؤسسات العامة وتشجيع الانفتاح.

وما يعنينا من هذا القانون هو الحماية التي قررها للمعلومات السـرية، بالمادة (10) والتي تنص على أنه (مع عدم الإخلال بالقوانين والأنظمة المعمول بها في المملكة بشأن حق الأشخاص الطبيعيين والاعتباريين في الحصول على ما يطلبونه من معلومات للمسئول أن يمتنع بقرار مسبب عن الكشف عما يأتي (أ- المعلومات المتعلقة بالأسـرار والوثائق المحمية بموجب أي قانون آخر.

ب-المعلومات المصنفة التي يتم الحصول عليها باتفاق مع دولة آخرى.

ج-المعلومات المتعلقة بالأسـرار الخاصة بالدفاع الوطني أو أمن الدولة أو سياستها الخارجية.

د- المعلومات الشخصية المتعلقة بسجلات الأشـخاص التعليمية أو الطبية أو حساباتهم أو تحويلاتهم المصرفية أو أسـرار مهنتهم.

هـ - المعلومات المتعلقة بالمراسلات ذات الطبيعة الشخصية والسـرية والتي تتم عبر البريد أو البرق أو الهاتف أو عبر أية وسيلة تقنية آخرى مع الجهات الحكومية والإجابات عليها.

و – المعلومات التي يؤدي الكشف عنها إلى التأثير في المفاوضات بين المملكة وأية دولة آخرى.

---

(1) نص هذا المشـروع بقانون منشورة على الموقع الإلكتروني لمجلس النواب البحريني www.nuwab.gov.bh

ز- المعلومات المتعلقة بالتحقيقات التي تجريها النيابة العامة أو الأجهزة الأمنية بشأن أية جريمة أو قضية تدخل في اختصاصها، أو تجريها السلطات المختصة للكشف عن المخالفات المالية أو الجمركية أو البنكية وذلك قبل انقضاء الدعوى العمومية ما لم تأذن الجهة المختصة قانوناً بالكشف عنها.

ح- المعلومات التي يؤدي الكشف عنها إلى الخلال بأي حق من حقوق الملكية الفكرية أو بالمنافسة العادلة أو المشروعة التي يترتب عليها تحقيق ربح أو خسارة بطريقة غير مشروعة لأي شخص أو شركة.

ط- المعلومات التي تتضمن مساساً بحقوق الآخرين المادية والمعنوية أو سمعتهم أو حرياتهم الشخصية.)

وتعكس هذه المادة حرص المشرع البحريني على كفالة الحماية للمعلومات السرية نظرا لما يترتب على إفشاء تلك السرية من المساس بالمصلحة العامة للدولة ومصلحة الأفراد.

3- مشروع بقانون بشأن حماية معلومات ووثائق الدولة[1]:

أحالت الحكومة هذا المشروع بقانون إلى مجلس النواب بشأن بموجب المرسوم رقم (118) لسنة 2011، حيث تم تصنيف المعلومات وفقا للمادة الثالثة منه إلى درجات وهي «سري للغاية» ويقصد بها (المعلومات والوثائق التي يؤدي إفشاء مضمونها إلى تهديد سلامة الدولة أو إلى حدوث أضرار بأمن الدولة أو مصالحها) ، ودرجة (سري) ويقصد بها (المعلومات والوثائق التي يؤدي إفشاء مضمونها إلى حدوث أضرار محدودة لأمن الدولة أو مصالحها)، ودرجة (محظور أو محدود) وهي (المعلومات والوثائق التي يؤدي إفشاء مضمونها إلى حدوث أضرار محدودة لأمن الدولة أو مصالحها). وقد نصت المادة الرابعة على أنه (مع مراعاة أي قانون آخر، تعتبر معلومات

(1) نص هذا المشروع بقانون منشورة على الموقع الإلكتروني لمجلس النواب البحريني www.nuwab.gov.bh

ووثائق الدولة الآخرى التي لا تشملها أحكام هذا القانون والقرارات الصادرة تنفيذاً لـه عادية، وعلى المسئول أن يحافظ عليها ويحفظها مـن العبـث أو الضـياع أو التلـف ولا يجوز إفشاء مضمونها لغير المعنيين بها). فيما تناولت المادة السادسـة حظـر إفشـاء أيـة معلومات أو وثائق محمية وفق هذا القانون ومنع تخزينها خارج الجهـة المعنيـة. وقـد بينت باقي المواد العقوبات التي توقع من ينتهك تلك الأسـرار

4-مشـروع قانون بتعديل بعض مواد قانون العقوبات البحريني[1]:

قدم هذا المشـروع بقانون إلى مجلس النواب البحريني في دور الانعقاد الأول من الفصل التشـريعي الثالث في عام 2011 والمتضمن تعديل بعض مـواد قـانون العقوبات البحريني لسنة 1976 والتي من بينها المـادة (372) والتـي تـنص عـلى أنه (يعاقب بالغرامة التي لا تجاوز عشـرين دينارا من فض رسالة أو برقيـة بغـير رضـا مـن أرسـلت إليـه أو اسـترق السـمع في مكالمـة تليفونيـة .ويعاقـب الجـاني بالحبس مدة لا تزيد على ستة أشهر أو بالغرامة التي لا تجاوز خمسين دينارا إذا أفشى الرسالة أو البرقية أو المكالمة لغير من وجهت إليه ودون إذنه متى كان مـن شأن ذلك إلحاق ضرر بالغير).

والنص كما ورد في مشـروع القانون، ينص على أنه (يعاقـب بالغرامـة التـي لا تجاوز مائة دينار من فض رسالة أو برقية بغير رضـا مـن أرسـلت إليـه أو اسـترق السمع في مكالمة هاتفية. أو اطلع على أسـرار الغير عن طريق شـبكة المعلومـات أو أي وسـيلة مسـتحدثة. ويعاقـب بـالحبس مـدة لا تزيـد عـلى سـتة أشـهر أو بالغرامة التي لا تجاوز مائتي دينارا إذا أفشى ما اطلع عليه من أسـرار الغـير عـن طريق شبكة المعلومات أو أية وسيلة مسـتحدثة آخـرى أو الرسـالة أو البرقيـة أو المكالمة لغير من وجهت إليه ودون إذنه متـى كـان مـن شـأن ذلـك إلحـاق ضرر بالغير)

(1) المرجع نفسه.

وقد أخذ على هذه المادة أنها تضمنت إضافة لبعض وسائل انتهاك الحق في الخصوصية بالاطلاع على أسرار الغير من خلال شبكة المعلومات ، دون أي بيان للمقصود بشبكة المعلومات حيث توجد العديد من شبكات المعلومات سواء على المستوى الداخلي للملكة أو على المستوى العالمي، فضلاً عن أن انتهاك الحق في الخصوصية يمكن أن يقع بواسطة شبكات المعلومات أو أي وسيلة مستحدثة أو غيرها، ومن ثم فلا توجد حاجة لتجريم استخدام وسيلة محددة دون غيرها ، فما دامت حماية خصوصية أسرار الأفراد هو محل الحماية فإنه يتعين تقرير هذه الحماية بغض النظر عن وسيلة ارتكاب الجريمة[1].

وقد تم تعديل النص السابق لينص بعد التعديل على انه (يعاقب بالغرامة التي لا تقل عن مائة دينار من فض رسالة أو برقية بغير رضا من أرسلت إليه أو استرق السمع في مكالمة هاتفية. ويعاقب بالحبس مدة لا تزيد على ستة أشهر أو بالغرامة التي لا تجاوز خمسمائة دينار إذا أفشى الرسالة أو البرقية أو المكالمة لغير من وجهت إليه ودون إذنه.)

ونلاحظ أن النص بعد تعديله أضحى مشابه للنص الأصلي إلا باستثناء العقوبة التي أصبحت اشد مما كانت عليه في النص الأصلي.

ومن جانبي أرى أن مسألة حماية البيانات والمعلومات الخاصة أكبر من أن تشملها مادة واحدة، فليس خطر الإفشاء هو ما تتعرض إليه فقط، لذا أقترح الأخذ بأحد الخيارين، الأول: إضافة باب خاص بقانون العقوبات أو قانون المعاملات الإلكترونية تحت عنوان (حماية البيانات الخاصة) على غرار قانون المعاملات الإلكترونية العماني لسنة 2008 ، والثاني: سن تشريع خاص لهذا الغرض على غرار القانون المغربي رقم 08- 09 المتعلق بحماية الأشخاص

---

(1) مذكرة دائرة الشئون القانونية (هيئة التشريع والإفتاء القانوني) حالياً بشأن التعليق على الأقتراح بقانون بتعديل بعض مواد قانون العقوبات الصادر بالمرسوم بقانون رقم (15) لسنة 1976 - ص 4. (هذه المذكرة ضمن مرفقات هذا المشروع بقانون) المنشور على الموقع الإلكتروني لمجلس النواب البحريني www.nuwab.gov.bh

الذاتيين تجاه معالجة المعطيات ذات الطابع الشخصي وغيره من قوانين حماية البيانات في دول أوروبا وأمريكا التي سبق تناولها فيما تقدم من هذا البحث، وذلك على النحو الذي يكفل الحماية اللازمة لتلك البيانات وخاصة في مجال المعالجة الإلكترونية في مراحل جمعها وتخزينها ومعالجتها واسترجاعها ونقلها. ويكفل لها الضمانات والمبادئ الأساسية مثل؛ مبدأ المشروعية والنزاهة في جمع المعلومات ، مبدأ الصحة، مبدأ تحديد الغاية، ومبدأ الأمن المعلومات.

ومما تقدم، نستظهر اتجاه المشرع البحريني لتوفير الحماية للمعلومات وسريتها، واتخاذه عدة خطوات في هذا الاتجاه وإن كانت تتسم بنوعٍ من البطء، وهو يدفعنا إلى دعوة المشرع البحريني للإسراع في إصدار تلك القوانين لتحقيق الأمن المعلوماتي المنشود في المملكة.

الخاتمة

الحمدلله الذي بنعمته تتم الصالحات، وأحمده على أن وفقني في إتمام هذه الدراسة والتي تدور حول " الحماية الجنائية لسرية المعلومات الإلكترونية - دراسة مقارنة"

فمن خلال استعراض موضوع الحماية الجنائية لسرية المعلومات الإلكترونية من خلال تناول الجرائم المعلوماتية الماسة بسرية المعلومات الإلكترونية، من جيث التعريف بالجريمة المعلوماتية من حيث مفهومها، وخصائصها، وسمات المجرم المعلوماتي وفئاته، باعتبار أن الجرائم الماسة بسرية المعلومات الإلكترونية هي إحدى صور أو تطبيقات تلك الجرائم. وبيان ماهية سرية المعلومات الإلكترونية من خلال بيان مفهوم المعلومات وعناصرها وطبيعتها القانونية، وبيان صور الجرائم المعلوماتية الماسة بسرية المعلومات الإلكترونية وهي جريمة الدخول (الولوج)غير القانوني للنظام المعلوماتي ، وجريمة الاعتراض غير القانوني ، من حيث مفهوم تلك الجرائم وأركانها مع تسليط الضوء على موقف المشرع البحريني والقضاء من تلك الجرائم ,

ودراسة سبل مكافحة الجرائم الماسة بسرية المعلومات الالكترونية, من خلال التعاون الدولي والإقليمي لمكافحة الجرائم المعلوماتية، واستعراض صور هذا التعاون مثل المساعدة القضائية المتبادلة ومجالاتها، بالإضافة إلى تناول مجالات المساعدة المتبادلة الخاصة بمواجهة الجرائم المعلوماتية، وتسليم المجرمين.

وبعد دراسة أبرز الجهود التشريعية لحماية المعلومات الإلكترونية لمواجهة الجرائم الماسة على المستوى الدولي والإقليمي ممثلة في أبرز الاتفاقيات والقرارات الخاصة بحماية البيانات والمعلومات ومكافحة الجرائم الماسة بها، والجهود التشريعية الوطنية ممثلة في جهود التشريعات محل المقارنة ، وبعد

إلقاء الضوء جهود مملكة البحرين في مكافحة تلك الجرائم من خلال بيان أهم مشروعات القوانين المتعلقة بهذا المجال والتي تعكف السلطة التشريعية بالمملكة على دراستها ومناقشتها.

وبعد هذه الرحلة العلمية الشاقة عبر هذا الموضوع، يسرنا أن نضع بين يدي القارئ جملة الاستنتاجات التي استخلصناها من خلال دراستنا هذه, والاقتراحات والتوصيات التي نرى ضرورة العمل على تنفيذها كصورة من صور تنشيط العمل الكفاحي الفعال في مجال مكافحة الجرائم الماسة بسرية المعلومات الإلكترونية، وفيما يلي بيان ذلك:

أولا- النتائج:

1- إن الجرائم المعلوماتية بما فيها الجرائم الماسة بسرية المعلومات الإلكترونية مثل الدخول غير القانوني ، أو الاعتراض أو الالتقاط غير القانوني للبيانات والمعلومات، جرائم ذات خطورة عالية وتشكل تهديداً خطيراً للأمن الاجتماعي والاقتصادي والسياسي والعسكري لسائر لمجتمعات التي باتت تعتمد اعتمادًا كليًا على الأنظمة الإلكترونية ، نظراً لطبيعة وقيمة المعلومات والبيانات المستهدفة في تلك الجرائم, وللخسائر المالية الضخمة الناجمة عنها التي تقدر بمليارات الدولارات.

2- إن التحقيق في تلك الجرائم وكشف مرتكبيها يتطلب تأهيل تقني وفني عالي المستوى للمحققين ومأموري الضبط ، وجهات إنفاذ القانون بوجه عام.

3- إن التعامل مع تكنولوجيا المعلومات يتطلب الحذر الشديد، وإن قلة الوعي بالمخاطر الإلكترونية، وعدم الإلمام بأساليب الاختراق، وعدم استخدام برامج ووسائل حماية حديثة وذات كفاءة جيدة، فضلاً عن إحجام الضحايا عن تبليغ السلطات المختصة بالدولة بالجرائم التي تعرضوا لها، كلها عوامل مساعدة لزيادة الجرائم المعلوماتية ومحفزاً لمرتكبيها على التمادي في إجرامهم.

4- المجرم المعلوماتي غالباً هو شخص يتمتع بقدر جيد من الذكاء والعلم والمهارة في استخدام وسائل تكنولوجيا المعلومات، وفي بعض الأحيان لا يكون دافعه إجرامي أو بنية الأضرار بالغير، وإنما يكون بدافع التسلية والمغامرة، مثل الشباب وصغار السن الذي يقدمون على ارتكاب أفعال تشكل جرائم معلوماتية مثل اختراق النظم المعلوماتية بهدف التسلية والمغامرة والتنافس واستعراض قدراتهم ومهاراتهم في استخدام الحاسب الآلي أمام أقرانهم, وهو ما يتعين مراعاته من قبل المشرع عند سن تشريع خاص بالجرائم المعلوماتية , حيث أن هذه الفئة بحاجة إلى معالجة خاصة.

5- في ظل تطور تكنولوجيا المعلومات وتنامي الاعتماد عليها في معالجة وتخزين وتبادل ونقل لمعلومات عبر الشبكات الإلكترونية من مكان لآخر، أصبح أمن المعلومات غاية ينشدها جميع مستخدمي هذه التكنولوجيا, وتعد السرية أحد الأهداف الأساسية لأمن المعلومات بالإضافة إلى السلامة والتكامل والتوفر.

6- إن أمن المعلومات، يتحقق بضمان الأمن التقني بمعنى أمن الشبكات وأمن الأجهزة المستخدمة والأمن القانوني الذي يتحقق من خلال بنية تشريعية تكفل الحماية الجنائية للمعلومات الإلكترونية والنظم المعلوماتية من أي اعتداء أو خطر يهدد سلامتها وسريتها.

7- يعد الدخول غير القانوني من أبرز التهديدات التي تواجه المعلومات المعالجة إلكترونيا، وإنه بمثابة الشرارة الأولى أو البوابة لارتكاب غيره من الجرائم المعلوماتية، فضلاً عما يتسبب به من خسائر مادية كبيرة للمجني عليه، نتيجة ما قد ينجم عنه من إحداث ثغرات في النظام المعلوماتي للمعتدى عليه أو تعطيل أجزاء منه أو إعاقة خدمات النظام, وبالتالي فوات فرص الربح على مالك النظام أو الموقع المعتدى عليه, خاصة إذا ما كان شركة تجارية أو بنك.

8- بسط الحماية الجنائية لنظم المعلومات بغض النظر عن تمتعها بنظام حماية من عدمه، دون قصرالحماية الجنائية على المنظم التي يوفر لها مالكوها نظم حماية ويشملوها بتدابير أمنية، لتفادي إفلات المجرمين الذي يقومون بالاعتداء على خصوصية وسرية معلومات الآخرين من العقاب لمجرد كون النظم المعلوماتية التي وقع عليها الاعتداء غير مؤمنة بما يكفي من قبل مالكيها،وخاصة إذا لم يكن هناك التزام قانوني يلزمه بوضع برامج أو اتخاذ تدابير محددة لحماية النظام المعلوماتي، وحتى لو كان هناك مثل هذا الالتزام، فإن ذلك لا يعني عدم مجازاة المعتدي على حرمة النظام المعلوماتي نتيجة لإخلال المعتدى عليه بقواعد الحماية, وندعم رأينا هذا، بأنه في جريمة السرقة لا يؤثر تمتع المال المسروق بنوع معين من الحماية من قبل مالكه من عدمه على قيام جريمة السرقة.

9- تختلف التشريعات في تحديد مدى تحقق النتيجة الإجرامية في جريمة الدخول غير القانوني للنظام المعلوماتي،حيث ذهبت بعض التشريعات إلى الاكتفاء بمجرد الدخول إلى النظام المعلوماتي ، سواء نجح الجاني في الوصول إلى المعلومات أو البرامج المخزنة داخل النظام محل الجريمة أم لا، مثال القانون الخاص بحماية المعلومات في السويد الصادر عام 1973 وفرنسا والبرتغال، وقانون مكافحة جرائم تقنية المعلومات العماني لسنة 2011، قانون مكافحة جرائم تقنية المعلومات الإماراتي لسنة 2006, بينما تشترط بعض التشريعات الآخرى الوصول إلى المعلومات التي يتضمنها النظام المعلوماتي للقول بتحقق الدخول غير القانوني إلى النظام المعلوماتي، مثال القانون الفيدرالي الأمريكي لجرائم الحاسبات الآلية المادة 1030(a) (1) ، (2) ،ونظام مكافحة جرائم المعلوماتية السعودي لسنة 2007.

10- خلو قانون العقوبات البحريني والنصوص العقابية الأخرى الواردة في قوانين آخرى مثل قانون الاتصالات أو قانون المعاملات الإلكترونية وغيرها، من نص يجرم أفعال الدخول غير القانوني أو البقاء غير

القانوني داخل النظام المعلوماتي، أما بالنسبة لموقف القضاء البحريني فقد لجأ إلى تطبيق بعض النصوص التقليدية مثل نص المادة (290) من قانون العقوبات البحريني الخاصة بجريمة التسبب عمدا في إزعاج المجني عليها بإساءة استخدام الأجهزة السلكية واللاسلكية.

11- إن نصوص المواد (73) و(75) من المرسوم بقانون رقم (48) لسنة 2002بإصدار قانون الاتصالات اشتملت على صور حماية المراسلات الإلكترونية والتي تشمل جريمة الاعتراض غير القانوني للبيانات والمعلومات.

12- يقصد بجريمة الاعتراض غير القانوني للمعلومات أي نشاط غير مشروع يهدف إلى الاطلاع على محتوى اتصال من بيانات ومعلومات تتم داخل نظام حاسب آلي واحد، أو أكثر تربطها شبكة اتصالات باستخدام الوسائل الفنية التي تمكنه من ذلك.

13-اختلاف التشريعات التي تناولت جريمة الاعتراض غير القانوني للبيانات لاشتراط استخدام وسائل فنية في ارتكاب هذه الجريمة، وانقسمت إلى اتجاهين: الأول: لا يشترط استخدام وسائل فنية في ارتكابها مثل نظام مكافحة جرائم المعلوماتية السعودي لسنة 2007، والثاني: يشترط استخدام وسائل فنية في ارتكابها مثل اتفاقية بودابست المتعلقة بالجريمة الإلكترونية وقانون مكافحة جرائم تقنية المعلومات العماني لسنة 2011.

14- أثار التمييز بين بدء التنفيذ المعاقب عليه والأعمال التحضيرية غير المعاقب عليها إشكالية في نطاق جرائم المعلوماتية, حيث اختلفت الآراء بهذا الشأن، حيث ذهب رأي إلى مد النطاق العقابي ليشمل الأعمال التحضيرية التي تتداخل مع مفهوم الشروع، وذهب رأي منهم إلى أن الشروع يبدأ في اللحظة التي يذهب فيها الشخص لتشغيل الجهاز، بينما ذهب رأي آخر إلى أن الشروع هو مقدمة الفعل الجريمة وبالتالي فإن الجزء الأكبر من الأعمال التحضيرية يعد داخلا في نطاق الشروع المعاقب عليه، كما يرى البعض أن

إشكالية البدء في التنفيذ في الجرائم المعلوماتية تنبع بوجه عام في تحديد المعيار الذي يمكن الاعتماد عليه بالنسبة لهذه الجرائم, حيث يرون أن المعيار الشخصي لا يمكن الاعتماد عليه و يرجحون الاعتماد على المعيار المادي في الجرائم المعلوماتية, حيث يجعل الشروع في موقع أفضل عند عقد مقارنة بين الشروع والتلبس بالجريمة.

15- إن تحديد البدء بالتنفيذ في جريمة الدخول غير القانوني بقصد ارتكاب جريمة أخرى وهي جريمة ذات النتيجة التي يتصور فيها الشروع قد يثير إشكالية كبيرة، تتمثل في وحدة النشاط المادي بينها وبين جريمة الدخول غير القانوني المجرد وهي جريمة شكلية لا يتصور فيها الشروع ، فالسلوك المادي الذي يأتيه الجاني هو ذاته عند ارتكاب أي من الجريمتين, لذا نرى أن التمييز بين هاتين الحالتين يخضع للسلطة التقديرية لقاضي الموضوع الذي يمكنه استخلاص نية الجاني من ملابسات الواقعة والظروف المحيطة بها، كالاستدلال على نية الجاني في الدخول غير القانوني للحاسب الآلي بقصد الحصول على المعلومات ونسخها من خلال أدوات أو وسائط التخزين التي تكون بحوزته لحظة ضبطه.

16 يعتبر الفراغ أو القصور التشريعي أحد أهم التحديات الرئيسة في مجال مكافحة الجرائم المعلوماتية، وأخطر ما يمكن أن يترتب على ذلك إفلات مرتكبي هذه الجرائم من العقاب على الرغم مما يتسببون فيه من أضرار وخسائر ضخمة، وهو ما يشكل حافز لهم على استغلال هذا الفراغ لارتكاب المزيد من هذه الجرائم .

17- حرص المجتمع الدولي على توفير الحماية للمعلومات والبيانات بمختلف أنواعها وتبنى في سبيل ذلك عدد من الاتفاقيات والقرارات مثل الدليل الإرشادي لحماية الخصوصية ونقل البيانات الخاصة الصادر منظمة التعاون الاقتصادي والتنمية لعام 1980، قرار الجمعية العامة للأمم المتحدة 95/45 لسنة 1990 بشأن مبادئ توجيهية لتنظيم ملفات البيانات الشخصية المعدة بالحاسبة الإلكترونية.

18- تعد الدول الأوروبية والغربية منها تحديداً سباقة في مجال التشريعات الخاصة بالجرائم المعلوماتية وحماية البيانات والمعلومات المعالجة آليا، وذلك بحكم كونها أحد منابع ثورة المعلومات التي انطلقت إلى باقي دول العالم، وأولى الدول التي غاصت في بحور تقنيات المعلومات والاعتماد عليها بشكل كبير، وأولى الدول التي انكوت بنار تلك التقنية, ويمكن القول إنها انتهت من استكمال بنيتها التشريعية لحماية المعلومات ومكافحة الجرائم الواقعة عليها.

19- إن معظم الدول العربية لديها نقص أو تفتقر لوجود تشريعات متكاملة في مجال حماية المعلومات ومكافحة الجرائم الواقعة عليها ، كما تعاني من بطء في إجراءات إصدار القوانين الخاصة بالفضاء المعلوماتي بسبب تعدد الجهات المعنية بذلك.

20- على المستوى الإقليمي عملت الدول العربية من خلال جامعة الدول العربية على توحيد جهودها التشريعية في سبيل مكافحة الجريمة بشكل عام والجرائم المعلوماتية بما فيها الجرائم الماسة بسرية المعلومات الإلكترونية بشكل خاص ومن أبرز تلك الجهود, القانون الجزائي العربي الموحد1996،قانون الإمارات العربي الاسترشادي لمكافحة جرائم تقنية المعلومات وما في حكمها 2004، الاتفاقية العربية لمكافحة جرائم تقنية المعلومات 2010. وعلى المستوى الوطني، فإن هناك حراك تشريعي في عدد من الدول العربية نحو استكمال بنيتها التشريعية وسد ما بها من نقص لمكافحة الجرائم المعلوماتية وحماية المعلومات.

21- فيما يتعلق بمملكة البحرين فقد كفل الدستور والقانون نوعًا من الحماية الجنائية لسرية المعلومات، وذلك أما بمقتضى نصوص قانون العقوبات، مثال أسرار الدفاع، أو بموجب قانون خاص مثل قانون حماية الأسرار التجارية، أو بنصوص عقابية تضمنتها بعض التشريعات بمناسبة

تنظيم موضوع معين مثل القانون الخاص بالإحصاء والتعداد, إلا إنها أيضاً وكما سبق ذكره بالنسبة لمعظم الدول العربية, فإنها تعاني من نقص في البنية التشريعية في مجال حماية المعلومات ومكافحة الجرائم الواقعة عليها، فضلاً عن معاناتها هي الأخرى من بطء في إجراءات إصدار القوانين الخاصة بالفضاء المعلوماتي, وهذا لا يمنع من القول من أنها قد خطت خطوات متقدمة في سبيل استكمال بنيتها التشريعية وسد ما بها من نقص لمكافحة الجرائم المعلوماتية وحماية المعلومات من خلال عدد من المشروعات بقانون الخاصة بمكافحة جرائم الحاسب الآلي وحماية أسرار ومعلومات ووثائق الدولة المعروضة على السلطة التشريعية بالمملكة.

ثانياً: التوصيات

1- نشر ثقافة التعامل الآمن والسليم مع تكنولوجيا المعلومات بين أفراد المجتمع، بحيث تتضمن الأتي:

أ التوعية بفوائد وأهمية تكنولوجيا المعلومات في تنمية الفرد والمجتمع والمجالات الصحيحة لاستخداماتها.

ب التوعية بمخاطر استخدام وسائل تكنولوجيا المعلومات وشبكات الاتصال، وأساليب الاختراق وكيفية قيام قراصنة الإنترنت مثلا باستهداف ضحاياهم لسرقة البيانات أو المعلومات الخاصة بهم واستخدامها لأغراض تخدم أهدافهم الإجرامية، وكيفية اكتشاف تعرض أجهزتهم لعمليات اختراق.

ج- التوعية بالوسائل التي تحقق لهم الاستخدام الآمن، وضرورة استخدام برامج ووسائل حماية حديثة وذات كفاءة جيدة، مع مراعاة تحديثها بصورة دورية.

د- التوعية بضرورة التبليغ السريع والفوري عن حوادث الاعتداء التي يتعرضوا لها من عمليات اختراق أو التقاط المعلومات أو غيرها من

الاعتداءات، حتى تتمكن الجهات المختصة بمكافحة الجرائم، من سرعة تتبع مرتكبي تلك الجرائم والتحفظ على الأدلة المتحصلة عنها والتي تتسم بسرعة الزوال.

2- ضرورة إحاطة المشتغلين بالقانون والقضاء بالحد الأدنى من المعرفة الفنية التي تساعدهم على فهم الجريمة بشكل أعمق وأوضح.

3- اقترح على الجهات المختصة بالمملكة العمل بصورة مستمرة على تطوير الجهاز القائم لمكافة الجرائم الإلكترونية التابع للإدارة العامة لمكافحة الفساد والأمن الإلكتروني والاقتصادي بوزارة الداخلية، وتزويده بأحدث الوسائل والأجهزة التقنية المتطورة وذات الكفاءة العالية، وتزويده بالعناصر البشرية المدربة ذات الخبرة الفنية والتقنية المؤهلة للتعامل مع هذا النوع من الجرائم والأدلة المتحصلة عنها وتتبع واكتشاف مرتكبيها, والحرص على أن يكون من بين اختصاصات هذا الجهاز الآتي:

أ- تلقي بلاغات الأفراد والمؤسسات والهيئات التي تقدم مباشرة، أو عن طريق الهاتف، أو عن طريق الفاكس أو البريد الإلكتروني، أو الموقع الإلكتروني التابع لهذا الجهاز والمخصص لتلقي البلاغات، وذلك كله مع ضمان السرية الكاملة لمقدمي البلاغات, والاستجابة الفورية والتعامل السريع مع تلك البلاغات.

ب- الانتقال السريع لمعاينة الأجهزة والمعدات محل الاعتداء وتجميع الأدلة وحفظها.

ج- حصر المواقع الإلكترونية المشبوهة المنتشرة على شبكة الانترنت مثل المواقع التي قد تشكل في حد ذاتها جريمة , كالمواقع التي قد تكون محرضة على ارتكاب تلك الجرائم ، أو تقدم المساعدة الفنية لمرتكبي هذه الجرائم من خلال الترويج لأفكار الاختراق أو تتيح لروادها استخدام برامج الاختراق، والفيروسات المدمرة للنظم والمعلومات, والعمل على تتبع جهة المصدر، والأشخاص القائمين عليها، وذلك تمهيداً على حظرها وملاحقة المسئولين

عنها جنائياً.

د- دراسة المصادر المختلفة للبرامج الخبيثة والمضرة, مسبباتها وأساليبها المتنوعة، اكتشاف أنواعها الجديدة، وأحدث أنواع الهجمات الإلكترونية , والمواقع الإلكترونية غير الآمنة والتي تستخدم كمصيدة للمستخدمين للحصول على معلوماتهم الخاصة، وعمل جداول دورية بتلك البرامج والمواقع تعمم على الجهات المختلفة بالدولة، وتنشر للعامة لتفادي التعامل معها.

ه- التنسيق مع الجهات الدولية والإقليمية والدول الأخرى في مجال مكافحة الجرائم المعلوماتية وتبادل المساعدة الفورية من أجل إجراء التحقيقات المتعلقة بالجرائم المعلوماتية، و تجميع الأدلة، والتحفظ على البيانات، وتقديم المشورة الفنية, وهذا الاختصاص تحديداً نستمده من المادة الثالثة والأربعون من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات 2010 الموقعة عليها مملكة البحرين والمادة الخامسة والثلاثون من اتفاقية بودابست المتعلقة بالجريمة الإلكترونية 2001، واللتين نصتا على أن تقوم كل دولة طرف بإيجاد جهاز متخصص يعمل على مدار الساعة يختص بتلك الأمور.

و- التنسيق مع الجهات الدولية والإقليمية وبالدول الأخرى بشأن تبادل المعلومات والبيانات بشأن مرتكبي الجرائم المعلوماتية، والمجرمين المطلوبين للمملكة.

ز- التنسيق مع الجهات الدولية والإقليمية والدول الأخرى بشأن التحقيقات المشتركة التي تتم بمناسبة إحدى الجرائم المعلوماتية.

4- نظراً لكون الجرائم المعلوماتية تعد أبرز نماذج الجرائم التي يشكل التعاون الدولي ركيزة أساسية في مكافحته، فإنني أقترح قيام مملكة البحرين وجميع الدول العربية بالانضمام إلى اتفاقية بودابست المتعلقة بالجرائم الإلكترونية 2001، حيث إنه متاح لكافة الدول الانضمام إليها، طالما أنها

تتضمن ذات المبادئ التي تضمنتها الاتفاقية العربية لمكافحة الجرائم المعلوماتية 2010 الموقعة من معظم الدول العربية، وما تتمتع به من قبول واستحسان عالمي ، وذلك بغية توسيع نطاق التعاون الدولي في مجال مكافحة الجرائم المعلوماتية، خاصة وأن كثيراً من الهجمات الإلكترونية مصدرها الدول الأوروبية والولايات المتحدة الأمريكية، فضلاً عن الاستفادة من تجارب وخبرات تلك الدول في هذا المجال.

5- قيام جامعة الدول العربية بإنشاء شبكة عربية لها نقاط اتصال وطنية في كل دولة عربية متخصصة بالجرائم المتصلة بالتكنولوجيا والمساعدة على التحقيق فيها على غرار شبكة المعلومات التابعة لمجموعة دول الثمانية، تضم المتخصصين القادرين على توفير التعاون التقني في مجال مكافحة الجريمة بمجالات التكنولوجيا الرفيعة في صفوف الأجهزة الأمنية , وإعداد طرق لمتابعة الهجمات على شبكات الحاسبات الإلكترونية واكتشاف المتسللين خلال أقصر وقت، وإجراء تحقيقات في الدول التي يختفي فيها متهمون في حال عدم إمكانية تسليمهم، وإعداد طرق جديدة لاكتشاف ومنع جرائم الحاسبات الإلكترونية،واستخدام التكنولوجيا التي تسمح بالحصول على شهادات شهود من الدول الآخرى، الأمر الذي يشكل دعماً كبير للدول العربية في مكافحة تلك الجرائم من جهة، وكجهة تنسيق بين الدول العربية بعضهم البعض، وبينهم وبين باقي المنظمات العالمية والإقليمية الأخرى في ذات المجال, لما لذلك من فائدة إقليمية وعالمية، فزيادة أجهزة مكافحة الجرائم المعلوماتية، هو زيادة في تضييق الخناق على مرتكبيها.

6- لما كان قانون الإمارات العربي الاسترشادي لمكافحة جرائم تقنية المعلومات وما في حكمها 2004 مثال هام على التعاون الإقليمي والدولي لمكافحة الجرائم المعلوماتية، ولما كان قد تم إعداده ليكون بمثابة نموذج أو دليل تسترشد به كل دولة عضو بالجامعة العربية عند سنها تشريعاً وطنياً خاص بمكافحة الجرائم المعلوماتية، وفرصة لتبادل الأفكار في هذا

المجال.لذا أقترح إعادة طرح هذا القانون النموذجي للمناقشة من قبل الجهات المختصة بالجامعة العربية مثل مجلسي وزراء العدل والداخلية العرب، لإعادة النظر فيه وإجراء التعديلات اللازمة عليه في ضوءالاتفاقية العربية لمكافحة جرائم تقنية المعلومات 2010، كما نقترح أن يكون هذا القانون النموذجي حاضراً بشكل دوري على طاولة اجتماعات المختصين بالدول العربية لمراجعته بشكل مستمر وإدخال التعديلات اللازمة عليه بما يجعله نموذجاً متطوراً بقدر التطور السريع الذي تتسم به هذه الجرائم المعلوماتية.

7- اقترح على المشرع البحريني الآتي:

أ- اقترح على المشرع البحريني تعديل المادة (75) من المرسوم بقانون رقم (48) لسنة 2002 بإصدار قانون الاتصالات بحيث تشمل تجريم التقاط وتسجيل المعلومات والبيانات التي تتعلق بمضمون أية رسالة أو بمرسلها أو بالمرسل إليه.

ب- إعادة النظر في المشروع بقانون الخاص بجرائم الحاسب الآلي في ضوء الملاحظات التي سقناها في متن البحث بمناسبة التعليق على هذا المشروع.

ج- بالنسبة لجريمة الدخول غير القانوني، أن يشمل بالتجريم مرحلة المحاولة وهي تلك المرحلة التي تلي مرحلة الأعمال التحضيرية وتسبق البدء بالتنفيذ، وذلك بالنسبة للنظم المعلوماتية الخاصة بالمؤسسات الحكومية والأمنية، والدفاع، والنظم المعلوماتية الخاصة بالبنوك والمؤسسات المالية، وبنوك المعلومات، لتحقيق قدرا أكبر من الحماية لتلك النظم التي تتضمن معلومات تهدد أمن واستقرار الدولة من الناحية الأمنية والعسكرية والاقتصادية وذلك للمبررات التي سقناها بمناسبة تناول مسألة تحديد البدء في التنفيذ في الجرائم المعلوماتية في متن هذا البحث.

د دمج مشاريع القوانين المتعلقة بحماية معلومات مثل المشروعات

بقوانين بشأن حماية معلومات ووثائق الدولة والمشروع بقانون بشأن ضمان حق الحصول على المعلومات، في مشروع قانون واحد، مع اقتراح أن يضاف إليه جزء خاص يتعلق بحماية البيانات الخاصة، ليكون مسمى المشروع بقانون الجديد (مشروع بقانون بشأن حماية المعلومات وتنظيم حق الحصول عليها) على أن يقسم هذا المشروع الجديد إلى عدة أبواب على النحو الأتي:

-الباب الأول: أحكام عامة

- الباب الثاني: حماية معلومات ووثائق الدولة
- الباب الثالث: حماية البيانات الخاصة
- الباب الرابع: تنظيم حق الحصول على المعلومات
- الباب الخامس: العقوبات

وذلك لوحدة الموضوع والهدف من تلك المشروعات بقوانين وهو حماية المعلومات والبيانات كافة وتنظيم الحصول عليها، بغية إيجاد مرجع واحد خاص بحماية البيانات يسهل الرجوع إليه.

د- تبني فكرة العقوبات البديلة لبعض فئات مجرموا المعلوماتية خاصة من الشباب وصغار السن الذين لا يكون لديهم دافع إجرامي أو نية الأضرار بالغير، بعبارة أخرى تقل لديهم الخطورة الإجرامية ، وإنما يقومون بذلك بدافع التسلية والمغامرة، والتنافس واستعراض قدراتهم ومهاراتهم في استخدام الحاسب الآلي أمام أقرانهم. وتبرير ذلك أن للخطورة الإجرامية دورا هاماً في النظم الجنائية الحديثة، حيث أن الغرض من العقوبة لم يعد قاصرا على توقيع الجزاء على مرتكب الجريمة لردعه، بل يتعداه إلى غرض آخر وهو إعادة إصلاح المجرم وتأهيله، وبما أن مرتكبي الجرائم تتفاوت لديهم درجة هذه الخطورة تبعاً لأحوالهم النفسية والظروف المجتمعية المحيطة بكل منهم، مما يستوجب تبعا لذلك اختيار الجزاء الملائم بالنسبة لكل واحد منهم بغية تحقيق الغرض الحقيقي للجزاء وهو إصلاح المجرم، ولما كان الهدف من

العقوبات البديلة الحيلولة دون دخول تلك الفئة قليلة الخطورة الإجرامية السجن أو مركز الإصلاح لتفادي عيوب العقوبات سالبة الحرية قصيرة المدة التي تفوق أضررها منافعها لأنها تؤدي إلى اختلاط المحكوم عليه خلال هذه المدة القصيرة بالمجرمين المخضرمين المحترفين للإجرام داخل المؤسسات العقابية، الأمر الذي قد يؤدي إلى انتقال عدوى الإجرام إلى هؤلاء صغار السن أو الشباب، فيتعلمون فنوناً جديدة من الإجرام خاصة, وبالتالي زيادة خطورتهم الإجرامية بدلاً من إصلاحهم، فإنه يكون من الأنسب تبني فكرة العقوبات البديلة بالنسبة لهذه الفئة من مجرموا المعلوماتية.

وفي هذا المقام يمكن اقتراح مجموعة من العقوبات البديلة التي تتناسب مع هذه لفئة من المجرمين:

- إلزام المحكوم عليه بالعمل الإجباري ذي النفع العام مجاناً في المصالح الحكومية أياما محددة مع تحديد حد أدنى وأقصى لعدد الساعات، خلال مدة محددة لا تتعدى الستة أشهر مثلا أو السنة.

- يمكن اختيار الغرامات بأن يلزم المحكوم عليه بدفع مبلغ معين إلى الخزينة تحدده المحكمة مراعية عند تقديره جسامة الجريمة المرتكبة.

- إلزام المحكوم عليه بتدريب عدد معين من الأفراد ولمدة محددة من الساعات وخلال مدة محددة من السنة على استخدام تقنيات الحاسب الآلي،وفق رقابة و إشراف من الجهات المختصة , مما يساهم في محو أمية الحاسب الآلي, وتعزيز روح الاستخدام الإيجابي للمهارات والقدرات التي يملكها المحكوم عليه .

تم بحمدالله تعالى وعونه،،،

المراجع

أولا: الكتب الإسلامية:

1- الأشباه والنظائر لجلال الدين عبدالرحمن بن أبي بكر السيوطي، مطبعة مصطفى بأبي الحلبي- الطبعة الأخيرة 1378هـ

2- تفسير حقي (روح البيان في تفسير القرآن) لإسماعيل حقي البروسوي - - نسخة إلكترونية منشورة على الموقع الإلكتروني: http://islamport.com

3- تفسير القرآن العظيم للإمام الحافظ أبي الفداء إسماعيل إبن كثير دار الجيل بيروت ج4 (سنة النشر غير مذكورة)

4- حماية المال العام في الفقه الإسلامي للدكتور نذير بن محمد الطيب أوهاب أكاديمية نايف العربية للعلوم الأمنية - الرياض – الطبعة الأولى 2001

5- السلوك الاجتماعي في الإسلام للشيخ حسن أيوب - دار السلام للطباعة والنشر والتوزيع والترجمة – القاهرة 1996

6 فتح الباري بشرح صحيح البخاري للحافظ أحمد بن حجر العسقلاني – دار الفكر للطباعة والنشر والتوزيع – بيروت 1993 - ج12

7- موسوعة نظرة النعيم في مكارم أخلاق الرسول الكريم صلى الله عليه وسلم لصالح بن عبدالله بن حميد ، عبدالرحمن بن محمد بن ملوح - دار الوسيلة للنشر والتوزيع جدة الطبعة الأولى 1998

ثانياً: الكتب القانونية:

1. د.إبراهيم حامد طنطاوي، الحماية الجنائية لسرية معلومات البنوك عن عملائها في ضوء القانون رقم 88 لسنة 2003 دراسة مقارنة، دار النهضة العربية 2005

2. أبو الفضل جمال الدين محمد بن مكرم بن منظور، لسان العرب، مطبعة دار صادر- بيروت – الطبعة (1) سنة 1410 هـ- 1990

3. د. أحمد حسام طه تمام الحماية الجنائية لتكنولوجيا الاتصالات (دراسة مقارنة) - دار النهضة العربية 2002م

4. د. أحمد خليفة الملط – الجرائم المعلوماتية – دار الفكر الجامعي – الإسكندرية 2005

5. أحمد عوض بلال – مبادئ قانون العقوبات المصرى –القسم العام – دار النهضة العربية-القاهرة 2006

6. د.أحمد فتحي سرور - الوسيط في قانون العقوبات - دار النهضة العربية - القاهرة 1996

7. د.أيمن عبدالله فكري جرائم نظم المعلومات (دراسة مقارنة) دار الجامعة الجديدة للنشر – الإسكندرية 2007

8. بلال أمين زين الدين جرائم نظم المعالجة الآلية للبيانات في التشريع المقارن والشريعة الإسلامية – دار الفكر الجامعي - الإسكندرية 2008

9. د.جميل عبد الباقي الصغير، الجوانب الإجرائية للجرائم المتعلقة بالإنترنت، دار النهضة العربية، القاهرة 1998م

10. د.حسن طاهر داود – أمن شبكات المعلومات- معهد الإدارة العامة ، مركز البحوث، المملكة العربية السعودية 2004

11. د.خالد ممدوح إبراهيم – الجرام المعلوماتية – دار الفكر الجامعي – الإسكندرية 2009

12. د.ذياب البداينة الأمن وحرب المعلومات - عمان الأردن - دار الشروق 2002

13. د. رمسيس بهنام ، قانون العقوبات جرائم القسم الخاص ، منشأة المعارف ، الإسكندرية 1999

14. سامي علي حامد عياد الجريمة المعلوماتية وإجرام الإنترنت دار الفكر الجامعي الإسكندرية 2007

15. سراج الدين الروبي آلية الانتربول في التعاون الدولي الشرطي الدار المصرية اللبنانية الطبعة الثانية 2001

16. سراج الدين محمد الروبي الانتربول وملاحقة المجرمين الدار المصرية اللبنانية - القاهرة 1998

17. د.سليمان عبدالمنعم – النظرية العامة لقانون العقوبات – دار الجامعة الجديدة للنشر 2000 ا- الإسكندرية

18. د.صالح جواد الكاظم، مباحث في القانون الدولي- الطبعة الأولى- دار الشؤون الثقافية العامة - بغداد 1991

19. عبدالفتاح بيومي حجازي، النظام القانوني لحماية التجارة الالكترونية: الكتاب الثاني، الحماية الجنائية للتجارة الالكترونية، دار الفكر الجامعي الإسكندرية 2002

20. د.عبدالفتاح محمد سراج النظرية العامة لتسليم المجرمين دار النهضة العربية بدون تاريخ نشر - القاهرة

21. د.عبدالفتاح مراد شرح جرائم الكمبيوتر والانترنت شركة البهاء للبرمجيات والكمبيوتر والنشر الإلكتروني- الإسكندرية- سنة النشر- غير مذكورة

22. عبدالقادر عودة - التشريع الجنائي الإسلامي مقارنا بالقانون الوضعي دار الطباعة الحديثة - 1984 – ج1

23. عفيفي كامل عفيفي – جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون دراسة مقارنة منشورات الحلبي الحقوقية بيروت- لبنان

24. د.علي خليل إسماعيل الحديثي- القانون الدولي العام – ج (1) المبادئ والأصول – دار النهضة العربية – القاهرة 2010

25. د.عماد الصابغ نظم المعلومات (ماهيتها ومكوناتها) - دار الثقافة للنشر والتوزيع عمان- الطبعة الأولى 2000

26. د.عمر محمد أبوبكر بن يونس الجرائم الناشئة عن استخدام الإنترنت دار النهضة العربية - القاهرة – الطبعة الأولى 2004

27. د.عمرو إبراهيم الوقاد، الحماية الجنائية للمعلوماتية- بدون جهة أو تاريخ نشر، صـ 119

28. د.فوزية عبدالستار - شرح قانون العقوبات القسم العام النظرية العامة للجريمة- دار النهضة العربية 1992 القاهرة

29. د.فوزية عبدالستار - مبادئ علم الإجرام وعلم العقاب - دار المطبوعات الجامعية - الإسكندرية – 2007

30. د.محمد سامي الشوا – ثورة المعلومات وانعكاساتها على قانون العقوبات – دار النهضة العربية – القاهرة – الطبعة الثانية

31. محمد عبدالله أبو بكر سلامة – موسوعة جرائم المعلوماتية (جرائم الكمبيوتر والانترنت) – منشاة المعارف – الإسكندرية 2006

32. د.محمد محمد الهادي تكنولوجيا المعلومات وتطبيقاتها - دار الشروق - القاهرة الطبعة الأولى 1989م

33. محمود أحمد عبابنة جرائم الحاسوب وأبعادها الدولية دار الثقافة للنشر والتوزيع الأردن – عمان 2009

34. د.محمود شريف بسيوني، خالد محيي الدين - الوثائق الدولية والإقليمية المعنية بحقوق الإنسان – المجلد الثالث - دار النهضة العربية – القاهرة

35. د.محمود نجيب حسني ، شرح قانون العقوبات - القسم الخاص ، دار النهضة العربية - 1986

36. د.نائلة عادل محمد فريد قورة – جرائم الحاسب الاقتصادية (دراسة نظرية وتطبيقية) – دار النهضة العربية – القاهرة 2004/2003

37. نسرين عبدالحميد نبيه- الجريمة المعلوماتية والمجرم المعلوماتي- منشأة المعارف – الإسكندرية 2008

38. د.هشام محمد فريد رستم - قانون العقوبات ومخاطر تقنية المعلومات - 1995 مكتبة الآلات الكاتبة – أسيوط – مصر

39. د.هلالي عبداللاه أحمد الجوانب الموضوعية والإجرائية لجرائم المعلوماتية على ضوء اتفاقية بودابست الموقعة في 23 نوفمبر 2001 دار النهضة العربية القاهرة الطبعة الأولى 2003

40. د.هلالي عبداللاه أحمد كيفية المواجهة التشريعية لجرائم المعلوماتية في النظام البحريني على ضوء اتفاقية بودابست – دار النهضة العربية 2011- القاهرة

41. د.يحيي مصطفى حلمي - أساسيات نظم المعلومات - مكتبة عين شمس القاهرة 1998

42. د.يونس عرب - موسوعة القانون وتقنية المعلومات - دليل أمن المعلومات والخصوصية - جرائم الكمبيوتر والإنترنت - الجزء الأول ، منشورات إتحاد المصارف العربية ، الطبعة الأولى.

ثالثاً: رسائل الدكتوراه والماجستير

- رسائل الدكتوراه:

1. عبدالله بن حمد بن ناصر الغطميل - أحكام تلف الأموال في الفقه الإسلامي – رسالة دكتوراة مقدمة لجامعة أم القرى المملكة العربية السعودية 1408 هـ / 1988م

2. د.علاء عبدالباسط خلاف الحماية الجنائية للحاسب الإلكتروني والإنترنت في ضوء قانون العقوبات وقانون الاجراءات الجنائية وقانون حماية حقوق الملكية الفكرية بجمهورية مصر العربية- معهد الكويت للدراسات القضائية والقانونية- الطبعة الثانية 2008/2007

3. د.عمر أبو الفتوح عبدالعظيم الحمامي – الحماية الجنائية للمعلومات المسجلة إلكترونيا – دار النهضة العربية - القاهرة 2010

4. د. محمد على العرين ، الجرائم المعلوماتية كلية الحقوق جامعة الاسكندرية دار الجامعة الجديدة للنشر – الإسكندرية 2011

- رسائل ماجستير

1. قارة آمال - الجريمة المعلوماتية - رسالة ماجيستير جامعة الجزائر كلية الحقوق بن كعنون – السنة الجامعية 2001/ 2002

2. محمد أمين احمد الشوابكة جرائم الحاسوب والإنترنت (الجريمة المعلوماتية) دار الثقافة --عمان،الأردن 2004

رابعاً: الأبحاث والندوات والدوريات القانونية

1. الإرشاد الخامس - الجرائم السيبرانية ص 13 منشور على الموقع الإلكتروني http://isper.escwa.un.org/

2. بلفرد لطفي لمين التعاون الدولي في مجال تسليم المجرمين- مجلة الشرطة الجزائرية العدد 92 أكتوبر 2009

3. تقرير مؤتمر الأمم المتحدة الثاني عشر لمنع الجريمة والعدالة الجنائية سلفادور، البرازيل في الفترة من 12 إلى 19 أبريل 2010 – رمز الوثيقة A/CONF.213

4. تقرير مؤتمر المتابعة الإقليمية لمقررات القمة العالمية لمجتمع المعلومات 16-18 يونيو 2009 - دمشق - الأمم المتحدة - المجلس الاقتصادي والاجتماعي - اللجنة الاقتصادية والاجتماعية لغربي آسيا (الإسكوا)- رمز الوثيقة E/ESCWA/ICTD/2009/13

5. جان فرنسوا هنروت أهمية التعاون الدولي والتجربة البلجيكية في تبادل لمعلومات بين عناصر الشرطة والتعاون القضائي – برنامج تعزيز حكم القانون في بعض الدول العربية مشروع تحديث النيابات العامة - بحث مقدم بالندوة الإقليمية حول (الجرائم المتصلة بالكومبيوتر) في الفترة 19-20 نيسان / يونيو 2007 المملكة المغربية

6. جريدة أخبار الخليج البحرينية العدد رقم (12441) - الأحد 23 جمادى الأولى 1433هـ 15 أبريل 2012

7. جريدة الراية الاقتصادية القطرية الخميس 29 ربيع الآخر 1433 هـ - 22 مارس 2012م - العدد (10911)

8. د.حسام الدين الصغير ورقة عمل مقدمة بالاجتماع المشترك بين الويبو وجامعة الدول العربية حول الملكية الفكرية لممثلي الصحافة والإعلام - القاهرة، 23 و 24 مايو/ أيار 2005 - رمز المستند WIPO-LAS/IP/JOURN/CAI/05/2

9. د.حسين بن سعيد الغافري - الجاسوسية الرقمية - مقال منشور على الموقع الالكتروني: http://www.omanlegal.net/vb/showthread.php?t=442

10. د.حسين بن سعيد بن سيف الغافري - جرائم الحاسب الآلي ورقة عمل مقدمة من الأمانة العامة لمجلس التعاون الخليجي لاجتماع اللجنة الفنية المتخصصة بدراسة سبل مكافحة الجرائم الإلكترونية " الإنترنت" الأول والذي أنعقد بمقر الأمانة العامة بالرياض خلال الفترة من 4-2004/4/5م

11. راسل تاينر أهمية التعاون الدولي في منع جرائم الإنترنت - برنامج تعزيز حكم القانون في بعض الدول العربية مشروع تحديث النيابات العامة - بحث مقدم بالندوة الإقليمية حول (الجرائم المتصلة بالكومبيوتر) في الفترة 19-20 نيسان / يونيو 2007 المملكة المغربية

12. راسل تاينر - جرائم الإنترنت- التحدي لإنفاذ القانون- برنامج تعزيز حكم القانون في بعض الدول العربية مشروع تحديث النيابات العامة - بحث مقدم بالندوة الإقليمية حول (الجرائم المتصلة بالكومبيوتر) في الفترة 19-20 نيسان / يونيو 2007 المملكة المغربية

13. د.رقية عواشرية – نظام تسليم المجرمين ودوره في تحقيق التعاون الدولي لمكافحة الجريمة المنظمة- مجلة المفكر(مجلة علمية محكمة متخصصة في الحقوق والعلوم السياسية) جامعة محمد خضير- الجزائر – بسكرة – العدد الرابع 2008-

14. د.ضاري خليل محمود الشروع في الجريمة في قانون العقوبات البحريني المقارن فقها وقضاء – مجلة كلية الحقوق – جامعة البحرين – العدد الخامس مكرر شوال1429هـ - أكتوبر 2008

15. د.علي حسن الطوالبة- التعاون القضائي الدولي في مجال مكافحة الجرائم الإلكترونية- بحث منشور على الموقع الإلكتروني http://www.policemc.gov.bh/

16. فؤاد جمال - الجريمة الإلكترونية – جريدة الأهرام العربي – العدد 566 بتاريخ 2008/1/26 منشور على الموقع الإلكتروني: http://arabi.ahram.org.eg/

17. فتاوى دار الإفتاء المصرية الشيخ عطية صقر - مايو 1997 - راجع http://islamport.com

18. فهد عامر الأحمدي - كتيبة الفيروسات وجمعية الهكرز السعودي- مقال منشور بجريدة الرياض - العدد 14042 - الاثنين 13 ذي القعدة 1427هـ -4 ديسمبر 2006م

19. كريستينا سكولمان عن جرائم الإنترنت (طبيعتها وخصائصها- برنامج تعزيز حكم القانون في بعض الدول العربية مشروع تحديث النيابات العامة - بحث مقدم بالندوة الإقليمية حول (الجرائم المتصلة بالكومبيوتر) في الفترة 19-20 نيسان / يونيو 2007 المملكة المغربية

20. د.محمد البخاري بحث بعنوان تأثير الانترنيت على تطور المجتمعات 2010 منشور على الموقع الالكتروني: http://muhammad-2009.blogspot.com/2010/02/blog-post_27.html

21. د.محمد سامي الشوا، الغش المعلوماتي كظاهرة إجرامية مستحدثة، ورقة عمل مقدمة للمؤتمر السادس للجمعية المصرية للقانون الجنائي، القاهرة، 25-28 تشرين أول / أكتوبر 1993

22. ميرنا الحاج بربر- دراسة منشورة على الموقع الإلكتروني css.escwa.org.lb

23. النشرة الإعلامية COM/FS/2011-02/GI-03 الانتربول - http://www.interpol.com

24. ورقة عمل بعنوان (تدابير لمكافحة الجرائم المتصلة بالحواسيب) مقدمة في مؤتمر الأمم المتحدة الحادي عشر لمنع الجريمة والعدالة الجنائية بنكوك، 18 25 نيسان / إبريل 2005

25. ورقة عمل بعنوان (التطورات الأخيرة في استخدام العلم والتكنولوجيا من جانب المجرمين والسلطات المختصة في مكافحة الجريمة، بما في ذلك الجرائم الحاسوبية) مقدمة في مؤتمر الأمم المتحدة الثاني عشر لمنع الجريمة والعدالة الجنائية – سلفادور، البرازيل، 12- 19 نيسان / أبريل 2010

26. وسيم حرب - دراسة معتمدة من اللجنة الاقتصادية والاجتماعية لغربي آسيا (الإسكو) بالوثيقة رقم - E/ESCWA/ICTD/2007/8 بيروت 2007

27. د.يونس عرب - بحث بعنوان (صور الجرائم الإلكترونية واتجاهات تبويبها) هيئة تنظيم الاتصالات مسقط سلطنة عمان ورشة عمل تطوير التشريعات في مجال مكافحة الجرائم الإلكترونية 2-4 نيسان / إبريل 2006 منشور على الموقع الالكتروني /www ituarabic.org

28. د.يونس عرب - قراءة في الاتجاهات التشريعية للجرائم الإلكترونية مع بيان موقف الدول العربية وتجربة سلطنة عمان- ورقة عمل مقدمة بورشة عمل " تطوير التشريعات في مجال مكافحة الجرائم الإلكترونية " هيئة تنظيم الاتصالات / مسقط – سلطنة عمان 2-4 ابريل 2006

خامساً: الاتفاقيات والمعاهدات الدولية:

الاتفاقيات الدولية :

1. اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية 2000م
2. اتفاقية الجوانب المتصلة بالتجارة من حقوق الملكية الفكرية (اتفاقية التربس)
3. قرار الجمعية العامة للأمم المتحدة 95/45 لسنة 1990 بشأن مبادئ توجيهية لتنظيم ملفات البيانات الشخصية المعدة بالحاسبة الإلكترونية

الاتفاقيات الإقليمية:

1. اتفاقية تسليم المجرمين بين دول الجامعة العربية 1952
2. اتفاقية الرياض العربية للتعاون القضائي لعام
3. 1983 اتفاقية المجلس الأوروبي بشأن حماية الأفراد في مواجهة المعالجة الآلية للبيانات الشخصية 1981

اتفاقيات ثنائية :

1. اتفاقية التعاون القضائي والقانوني في المواد المدنية والتجارية والجزائية والأحوال الشخصية وتسليم المجرمين وتصفية التركات بين دولة البحرين والجمهورية العربية السورية لسنة 2001

2. اتفاقية التعاون القانوني والقضائي في المواد المدنية والتجارية بشأن الإعلان بالحضور و الأوراق القضائية والإنابات وتنفيذ الأحكام القضائية وأحكام المحكمين بين حكومة مملكة البحرين وحكومة جمهورية الهند لسنة 2005.

الاتفاقيات المتخصصة في مجال مكافحة الجرائم المعلوماتية :

1. اتفاقية بودابست المتعلقة بالجريمة الإلكترونية لسنة2001

2. الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010

القوانين النموذجية أو الإرشادية:

1. القانون العربي الاسترشادي للتعاون القضائي الدولي في المسائل الجنائية الإنابة القضائية.

2. القانون الجزائي العربي الموحد القانون.

3. القانون الاسترشادي الخاص بالجرائم المعلوماتية الصادر عن اللجنة الاقتصادية والاجتماعية لغربي أسيا (الإسكوا)

سادساً: القوانين

1- إنجلترا:

قانون إساءة استخدام الحاسبات الآلية الانجليزي لسنة 1990

– قانون حماية البيانات لسنة 1998 الانكليزي

2- الإمارات العربية المتحدة:

القانون الاتحادي رقم 2 لسنة 2006 في شأن مكافحة جرائم تقنية المعلومات

– قانون حماية البيانات الشخصية ٢٠٠٧ – دبي

3- البحرين:

– دستور مملكة البحرين.

– قانون العقوبات البحريني لسنة 1976

المرسوم بقانون رقم (7) لسنة 1977 في شأن الإحصاء والتعداد

- المرسوم قانون رقم (28) لسنة 2002 بشأن المعاملات الإلكترونية البحريني

المرسوم بقانون رقم (46) لسنة 2002 بإصدار قانون الإجراءات الجنائية

- المرسوم بقانون رقم (48) لسنة 2002بإصدار قانون الاتصالات

القانون رقم (7) لسنة 2003 بشأن حماية الأسرار التجارية.

قانون حماية المجتمع من الأعمال الإرهابية البحريني رقم (58) لسنة 20006

4- تونس:

قانون العقوبات التونسي لسنة 1913 المعدل بالقانون رقم 89 لسنة 1999.

5- الجزائر

- قانون العقوبات الجزائري1966 – وتعديلاته

6- السعودية :

نظـام مكافحة جرائم المعلوماتية السعودي لسنة 2007

7- سلطنة عمان:

قانون الجزاء العُماني

- المرسوم السلطاني رقم 72 / 2001 بتعديل قانون الجزاء العماني

المرسوم السلطاني رقم 2008/69 بإصدار قانون المعاملات الإلكترونية

المرسوم السلطاني رقم 12 لسنة 2011 بإصدار قانون لمكافحة جرائم تقنية المعلومات

8- السودان:

قانون المعاملات الإلكترونية لسنة 2007

قانون جرائم المعلوماتية لعام 2007

9- المغرب:

- القانون رقم 03-07 المتعلق بالإخلال بسير نظم المعالجة الآلية للمعطيات لسنة 2007

القانون رقم 08- 09 المتعلق بحماية الأشخاص الذاتيين تجاه معالجة المعطيات ذات الطابع الشخصي لسنة 2009

10- الولايات المتحدة الأمريكية:

- القانون الفيدرالي الأمريكي الخاص بإساءة استخدام الحاسبات الآلية

سابعاً: المعاجم ومراجع اللغة

1. الأسيل القاموس العربي الوسيط دار الراتب الجامعية الطبعة الاولى 1997 بيروت
2. Cambridge learner's Dictionary
3. مفردات ألفاظ القرآن للحسين بن محمد المعروف بالراغب الأصفهاني أبي القاسم - منشور على الموقع الإلكتروني /http://islamport.com
4. معجم الحاسبات – مجمع اللغة العربية - الطبعة الثانية الموسعة - القاهرة 1995

ثامناً: المواقع الإلكترونية

1. http://www.arab-ency.com/
2. http://www.justice.gov.ma/
3. http://ait.ahram.org.eg/
4. http://ar.hicow.com
5. http://ar.wikipedia.org
6. http://arabic.euronews.net
7. http://coeia.edu.sa/ar
8. http://isper.escwa.un.org
9. http://news.bbc.co.uk
10. http://saudialyoum.com
11. http://www.alarabiya.net
12. http://www.aljazeera.net
13. http://www.amanak.org
14. http://www.eurojust.europa.eu
15. http://www.gccpo.orgf
16. http://www.interpol.int/ar
17. http://www.islamstory.com
18. http://www.joradp.dz
19. http://www.law.cornell.edu
20. http://www.legislation.gov.uk
21. http://www.marefa.org

22. http://www.pcintv.com
23. http://www.tcl.jeeran.com
24. http://www.un.org/arabic
25. http://www.wisegeek.com
26. https://www.europol.europa.eu
27. www.arablawinfo com
28. www.nuwab.gov.bh
29. http://egyptjudgeclub org
30. http://www.cbos.gov.sd
31. http://www.coe.int
32. http://www.data.gov.bh
33. www.citc.gov.sa
34. http://www.ita.gov.om
35. http://www.arabipcenter.coms
36. http://www.aim-council.org/
37. http://www.arableagueonline.org
38. http://nauss.edu.sa
39. http://www.ita.gov.om
40. ,http://www.wipo.int/treaties/ar

الفهرس





٢١ شارع السعيد الشرقاوى - حى الجامعة
أمام القرية الأوليمبية - المنصورة
تليفون: ٠٥٠٢٢٣٦٢٨١ - محمول: ٠١٠٠٦٠٥٧٧٦٨
dar.elfker@hotmail.com

